Åbo Akademi
University

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 långsiktsplanering 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 samhälleliga 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 doktorstitel. 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 avhandlingsprocessen 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 nogsamhet 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

List of Figures (parts A & C)

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 bottlenecks[3] 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 phenomenons 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 arena[5]

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 lead 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 Treverton 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).

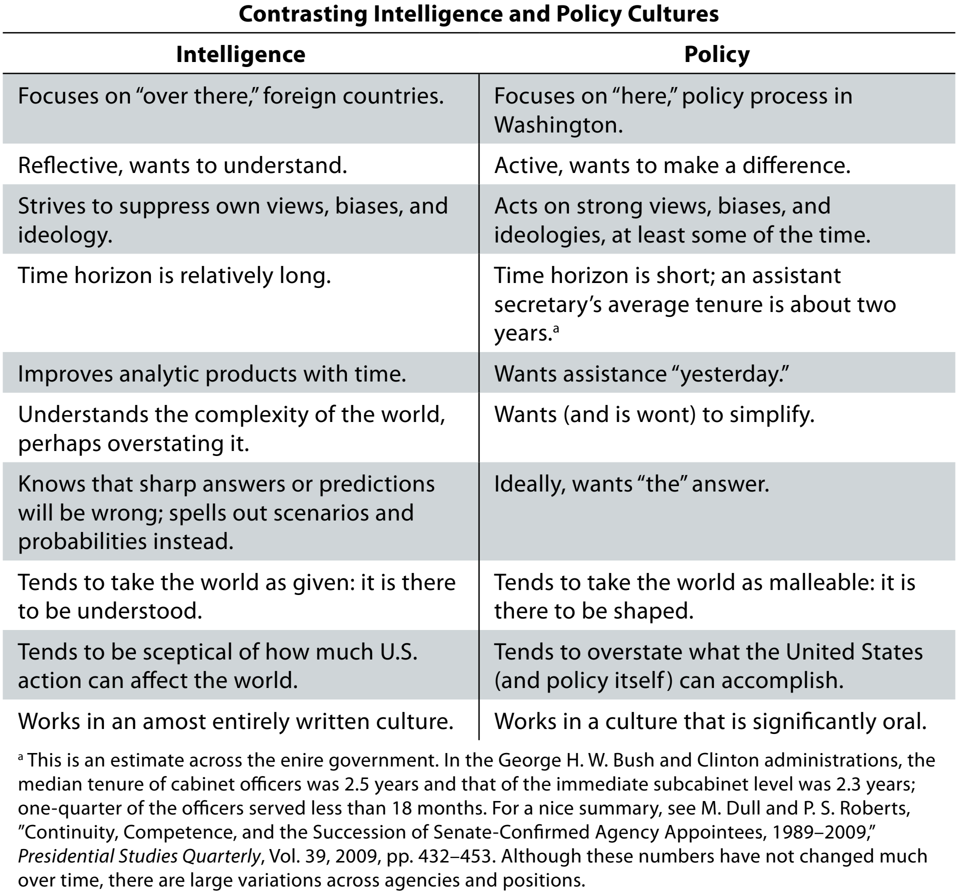
The links between the intelligence process and the policy process, and their different focuses, are described well in the table below (Treverton & Ghez, 2012). An important difference in the examination of the inertia in the decision chain and the link between intelligence and the policy process above 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 amost entirely written culture.	Works in a culture that is significantly oral.

[a] This is an estimate across the enire 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 deconflicted 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.

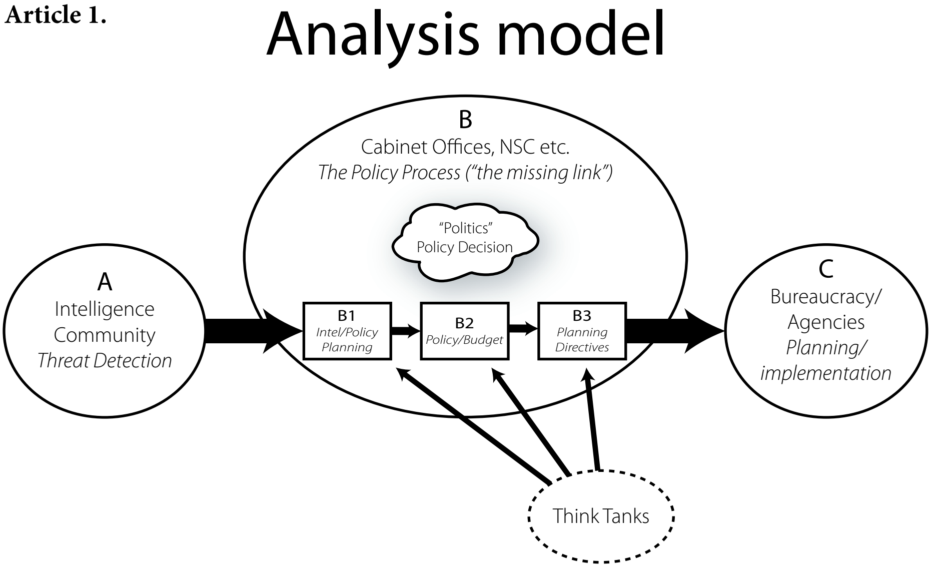


Figure 2: Analysis model Intelligence-Policy-Implementation

Country 1, 2, 3, 4[8]
Year 0 → Year N
Threat detection Implemented action

Country 5, 6
Year 0 → Year N-X
Threat detection Implemented action
Assignment: Illustrate/explain X

[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 agencies[10] 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.

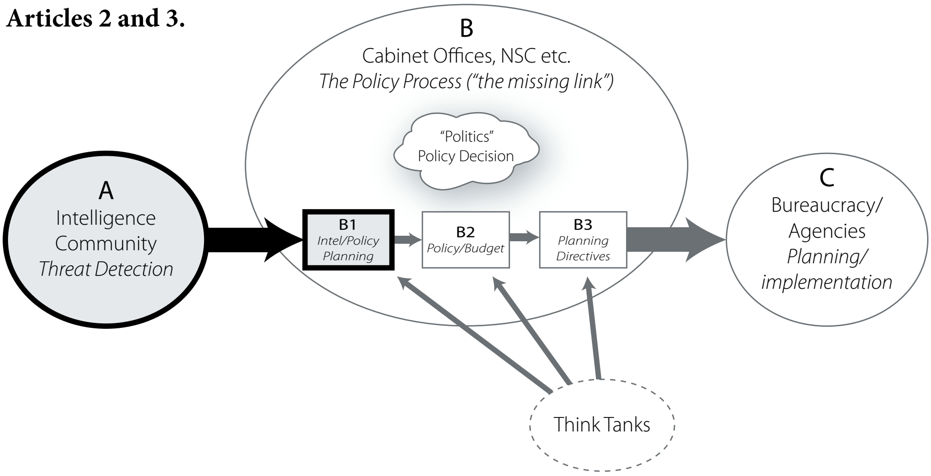


Figure 3: Relations Intelligence-Policy

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.

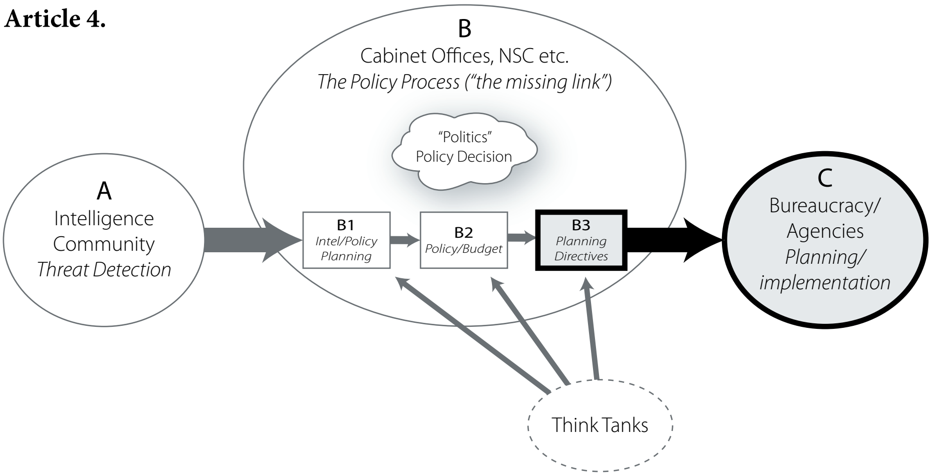


Figure 4: Relations Policy-Bureaucracy

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.

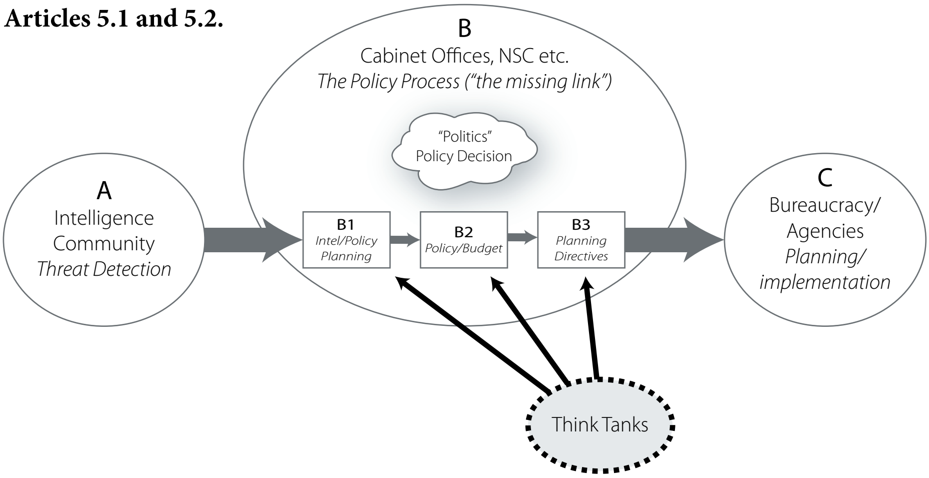


Figure 5: The impact of think tanks in the policy process

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". *Backgrounder* (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). "Självmordsbombaren fick 750 000 från CSN", 2013-02-18.
http://www.dn.se/nyheter/sverige/sjalvmordsbombaren-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 theoretisation 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/pccip/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

B. The articles

Article 1

Shielding the net

- understanding the issue of vulnerability and threat to the information society

Published 2010 in
Policy Studies
(Vol. 31, No. 3, May 2010, 283-300)
by Routledge

Abstract

This article looks at the policy processes of a number of different countries, from the realisation that a problem needs attention to the implementation of government policy. The event that initiates and drives the reform process of each country is tracked, revealing differences and similarities in urgency and perceived risks in the task of overhauling the legal framework for Critical Information Infrastructure Protection (CIIP). The final part of the article seeks to understand and account for those similarities and differences in policy implementation or in some cases, the lack of it.

The findings tend to suggest that there were lead countries that initiated the process of policy reform in CIIP, and this caused a number of other countries to follow suit. Although there are similarities in the trigger mechanism, which started the process, there was divergence in the passage of the recommendations and policy suggestions that resulted from the structure of the national governments and bureaucratic structures that has placed constraints upon the progress in some cases.

Results from the analysis reveal a number of cases, which reveal compromises and other strategies in an effort to push the reform through in a contested political process, where cooperation from government agencies is not necessarily forthcoming. Some of the reform processes have even stalled and are in a form of limbo from which they have not been able to gain any momentum.

Background and Introduction

This article seeks to address the issue of how countries approach the problem of how to protect information networks, through the process of formulating and enacting policy. The scope of the article includes the period from 1995 until 2002, which saw a great number of technological changes and developments as well as challenges in terms of protecting critical information infrastructure. Originally the intention was to cover a more contemporary period of development in this sphere, however, when work began it was soon discovered that progress after this period was at times stalled. Hence the focus of this article was constrained by this fact.

It should be noted at this point that this article is part of a larger project. Therefore, the focus shall be predominantly on the practitioner's perspective and empirically rich. Theoretical concerns and discussions will be treated more thoroughly at a later date. The core purpose of the theory and method in this article seek to support the hypothesis, with regard to policy formulation and implementation that the focus should not only concern the problem that is attempting to be solved (in this case CIIP), but an understanding of politics in governmental and bureaucratic circles needs to be understood and taken into account.

The approaches taken to the problem by; Australia, Finland, Norway, Sweden, United States and the United Kingdom are examined. These selected countries seem quite appropriate to study since they are all early starters and became “internet literate” but also represent a variation due to their constitutional systems. Milestones and timelines shall be established, with regard to:

- When were these issues identified?
- When was the decision made on approaching the problem?
- When were the policies/recommendations presented?
- When did the cabinet/parliament decide on how to respond to those recommendations?
- When were the policies chosen and the roadmaps implemented within the public and governmental structures?

However, these questions are tied to and influenced by a number of different issues concerning the shape and nature of national (and in some cases international) bureaucratic politics. These considerations include; institutional characteristics, understanding catalysts for change, the politics of administrative reform, and the problems associated with policy implementation.

Institutional design according to Peters (2005) is “the formation of institutions within rational choice is the conscious design of institutions. [...] In some ways the principal purpose of understanding institutions in this approach is to be able to manipulate the outcomes in subsequent rounds of design.” (Peters, 2005, p. 64) It is a matter of trying to manipulate the environment in order to introduce as much predictability and reduce as much uncertainty as possible. An alternative is the “successive limited comparisons” that is a series of contrasts against the characteristics of the rational model. This casts some doubt upon the assumption that actors behave ‘rationally’. In part the issue is problematic due to the fact that determining and understanding what is rational and what is not, is not clearly defined or maybe not clearly understood. (Allison, 1971, p. 154)

An aspect that can be overlooked, when the focus is centred upon ‘logical’ behaviour of individuals in institutions and organisations, is the role of the leadership in the direction and the life of an organisation or institution. A contested assertion, by William Niskanen, is that the leadership of governmental bureaucratic organisations use their authority and standing to “maximise personal utility, usually through instruments such as larger budgets and larger allocations of personnel.” And that these achievements are used in order to increase the personal prestige of the ‘bureau chief’ and greater material benefits. A similar model has been developed for political actors too, as legislators and those responsible for identifying and assigned tasks and responsibilities. According to the traditions in normative institutionalism, membership to an institution imposes limits upon the rationality of individuals. (Peters, 2005, pp. 55-56)[11] In other words there are certain stereotypical expectations and demands that are imposed upon positions in society.

Graham Allison argues that organisations are far from monolithic structures, even at the top, where competition and different agenda affect the logic and functioning of those institutions. Thus decisions and policies are not necessarily the result of 'pure' and logical though, but rather as the result of a bargaining process.[12] This implies that the most appropriate response to the problem is at times a political compromise, which has implications for meeting problems effectively. With these theoretical aspects in mind we will now see how these could be applied in an empirical context and how the policies of protecting modern information societies were developed in the selected countries.

Scoping and Framing the Problem

There is no universal definition of CIIP or CII, but there is an understanding of the consequences and what the task entails. It is "the protection of essential electronic information services, such as IT systems, electronic communications, and radio and television services". The Swedish Commission on Vulnerability and Security identified the following areas as being essential: air traffic control systems, electric power systems, financial systems, national command systems, and telecommunication systems. (Dunn & Wigert, 2004, p. 159)

There has been an evident shift in the scoping of CIIP with regard to the combination of time and events. During the period 1995-2002 the focus was centred on antagonistic cyber-threats, which is also the focus of this study. After 2002 there was a change to embrace an *All-Hazards* approach to the field. However, the pendulum seems to be swinging back somewhat again, after the cyber-attacks in Estonia, Lithuania and Georgia, and the lessons and perceptions that have been (and are being) drawn from these events.

This article is primarily concerned with how the 'protection bar' was raised against those individuals or groups, which with the knowledge and or support of another country seek to render their victim (another country) helpless through a concerted attack. It is also limiting the scope to look for changes at the Cabinet or central government level. The independent variables are thus the perceived threat, budget constraints etc, and the degree of institutional change is the dependable variable for this analysis.

Country Approaches and Analysis

The countries below are sorted approximately in the order of when the IT-vulnerability issue in respective information societies was raised. After the countries have been individually presented, a table is used as a ready means to high-

[11] William Niskanen is the President of the CATO Institute in Washington DC. According to normative institutionalism the constraints are mostly internalised by participants, but according to rational choice institutionalism the restraints are more externally based.

[12] Please see Allison, G. T. 1971. Essence of Decision: Explaining the Cuban Missile Crisis, New York, Harper Collins Publishers

light the similarities and differences of all the countries studied in one quick glance followed by an analysis.

Country Approaches

United States

Besides the earlier mentioned debate in the USA - which led to commissioning of the PCCIP - vulnerability of the electronic information infrastructure was also realized by the military when the Pentagon 1996 published a report titled *Information Warfare Defence*. O. Sami Saydjari, former computer security expert for the Pentagon and current President of the private company Cyber Defence Agency[13] went as far as to state: "The threat and vulnerabilities to our national infrastructure is serious, it's getting worse, and it's getting worse at an increasingly fast rate."[14]

In 1996, Executive Order (E. O.) 13010 was issued, which recognised the importance of dealing with the problem of physical threats and dangers associated with the development of the IT sphere. It is perhaps the first official step that acknowledges the risks and threats to critical information infrastructure.[15] This also brought about the establishment of the Presidential Commission of Critical Infrastructure Protection (PCCIP).[16] In 1997 the PCCIP released the report *Common Defence Against Uncommon Threats: The Federal Role in Critical Infrastructure Protection*. A key message of the report was that the time to act was now and not to wait.[17] This call seemed to give an impetus to the goal of CIIP.

The Presidential Decision Directive 63 (PPD-63), of 22 May 1998, of President Bill Clinton designed to ensure protection of the critical infrastructure created a number of new organisational structures to facilitate this objective.

The overall coordinating body for the implementation of PDD-63 was the **National Coordinator for Security, Critical Infrastructure and Counter-terrorism**, which were under the auspices of the White House National Security Council staff. The official in charge was Richard Clarke - a high-profile person on the top of the system that was built up with a very high momentum.[18] To support him he had the **Critical Infrastructure Assurance Office** - an inter-agency office based with the Commerce Department, but also dual-hutted as

[13] See the web site of the organisation at - http://www.cyberdefenseagency.com.

[14] Bruno, G., *Backgrounder: The Evolution of Cyber Warfare*, The New York Times, www.nytimes.com, 27 February 2008

[15] Schulze, T. May/June 2006. CIIP – Reached its Peak?, European CIIP Newsletter, Vol. 2, No. 2, p. 18

[16] For detailed account of the activities of the PCCIP please refer to - http://cipp.gmu.edu/clib/PCCIPReports.php.

[17] Common Defence Against Uncommon Threats: The Federal Role in Critical Infrastructure Protection, Report of the President's Commission on Critical Infrastructure Protection, 1997

[18] Pat Milton, *Anti-terrorism Tsar savours challenge,* The Associated Press, 11 October 1998

a staff element for the White House. It assisted in the drafting of the National Plan for Information Security Protection; helps Federal agencies in assessing their CI dependencies and interdependencies; coordinates education, awareness and outreach programmes. Information-sharing with the private sector was also a significant element here.

There were a number of agencies and committees that dealt with other tasks set by PDD-63.[19] The most notable innovation here was the **National Infrastructure Protecting Centre (NIPC)** which was an operational joint venture body between Department of Justice (DoJ) and Department of Defence (DoD) that was housed in the FBI Headquarter building and manned by both FBI and DoD-personal. It was always an FBI-person who was the head but with a two-star general from DoD as his deputy.

There has been a steady policy programme of building up CIIP, beginning with PDD-63, E.O. 13231 (later revised by E. O. 13286) from 1 March 2003, the 2003 National Strategy to Secure Cyberspace and the related National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, and the HSPD-7 Directive on Critical Infrastructure Identification, Prioritisation and Protection (17 December 2003).[20] There has been a flurry of activity to try and update and coordinate the protection of CIIP assets. This activity is being matched in creating the bodies responsible for the protection too.

The current threat to the critical infrastructure is well recognized, and ways and means are trying to be devised to ensure its protection against attack. The Bush administration in November 2007 requested that the National Security Agency and the Department of Homeland Security coordinate with each other in order to protect government and civilian communication networks from hackers. Then in January 2008 President Bush signed two presidential directives that urged the creation of a comprehensive national cyber security initiative.[21]

The debate on the vulnerabilities of the information society and antagonistic threats started around 1993 and became a priority on the domestic political agenda – notably during the Clinton administration. The developments here have been thoroughly monitored by the rest of the leading information societies around the world. In terms of the initiation of the CIIP process, the United States was among the leading nations. Given the nature of the governmental bureaucracy, it could be expected to take longer than it did. This gives an indication to the high priority assigned to the task at all levels.

[19] *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities*, January 2001, pp. 4-5
Please see pages 3-7 of the document for a complete list of agencies and committees and their function.

[20] Bloomfield (Jr), L. P. May 2004. *Building an International Critical Infrastructure Protection Policy*, The CIP Report, Vol. 2, No. 11

[21] Bruno, G., Backgrounder: The Evolution of Cyber Warfare, The New York Times, www.nytimes.com, 27 February 2008

United Kingdom
The importance of Critical national Infrastructure (CNI – equivalent term of CIIP) according to the British perspective, which is tied to "the continuity is so important to national life that loss, significant interruption, or degradation of the service would have life-threatening, serious economic or other grave social consequences for the community or would be of immediate concern to the government." (Dunn & Wiegert, 2004, p. 185) ICT its importance are attached to the economic reforms of the 1980s and the early 1990s, where high-tech growth has replaced the former heavy industry focus.[22] Thus ICT and its well-being is in effect a centrepiece to the economic well-being of the UK. There are two perceived types of threat to CNI in the UK; one from terrorist attack (i.e. a physical attack), and an electronic attack on information and electronic systems (i.e. a virtual or cyber-attack).

The Information Warfare responsibility moved from the Ministry of Defence to the Cabinet Office and became a civilian issue in 1997. Legislation was implemented at an early stage in the UK in 1990 the Computer Misuse Act was introduced. Although an act, this legislation was much more as it not only tried to anticipate new and emerging potential threats, but also sought to head them off. It set out a number of crimes relating to committing crime with or to ICT systems, and prescribed the punishments for those transgressions. This was updated in 2006 with the Police and Justice Bill, which also seeks to bring UK legislation in line with the Council of Europe's Convention on Cybercrime. (Abele-Wiegert & Dunn, 2006, pp. 306-09)

In July 1996 the National Criminal Intelligence Service (NCIS) launched Project Trawler, which was a study into computer crime. A report from the project, *Crime on Information Highways*, was released in 1999. Computer crime was defined in the report as "an offence in which a computer network is directly and significantly instrumental in the commission of a crime. Computer interconnectivity is the essential characteristic."[23] NCIS was later tasked by the Association of Chief Police Officers to design a nationally coordinated high-tech crime strategy that could lead to the establishment of a high-tech crime fighting unit by April 2001.[24]

In 1998 the approach to information society was established by the Department of Trade and Industry Competitiveness *White Paper*. It duly noted the role that ICT played in promoting economic growth. This was followed in September 1999 with the report *e-commerce@its.best.uk* by the then Performance and Innovation Unit (now the Cabinet Office's Strategy Unit). It recommended an organisational and policy framework for attaining the goals outlined in the White Paper. These recommendations have since been implemented under the national strategy *UK Online*. (Dunn & Wiegert, 2004, p. 186) As with a number

[22] *UK Policy Developments*, IAAC Briefing Paper, No. 2, 27 April 2000

[23] *The Virtual Horizon: Meeting Law Enforcement Challenges*, Scoping Paper, Australasian Centre for Policing Research, Payneham (Australia), 2000, p. 72

[24] *Ibid.*, p. 73

of other countries in this study, the UK strategy involves understanding and protecting the vulnerable CII on the one hand, and on the other to promote and expand information society.

The formation of agencies, tasked with protecting the UK from electronic attack, began in Parliament in 1999. In 2001 two different bodies were established. First the National Infrastructure Security Co-ordination Centre (NISSC) was created as an entity attached to the British Security Service (MI 5), and secondly the Civil Contingencies Secretariat (CCS) within the Cabinet Office which should prepare for all contingencies besides "electronic attack". Then in 2007 NISSC had physical protection merged, all threats evolving from electronic attack and terrorism were merged in to the Centre for the Protection of National Infrastructure (CPNI).[25]

Part and parcel with CIIP is the necessity to have a national strategy and a coordinating body for that strategy. A *Government Information Assurance Strategy* was produced, which covers counter-terrorism strategies, national security concerns, and efforts directed against high-tech crime. The aim of the strategy is to convey the perception that measures are being taken to secure the information society as a means to instil confidence in ICT and the authorities.

Central Sponsor for Information Assurance (CSIA) is the coordinating body for the strategy, and works with government agencies. (Dunn & Wiegert, 2004, p. 186) CSIA was established within the Cabinet Office on 1 April 2003. In 2004 the agency produced a document, *Protecting Our Information Systems – Working in Partnership for a Secure and Resilient UK Information Infrastructure*. This paper deals with the government's approach to different risks and threats that challenge the security of information systems across the UK. (Abele-Wiegert & Dunn, 2006, pp. 300-01) The approach taken is proactive by the authorities, whose chief aims seem to be related to the task of firstly, prevention and then to considerations of mitigation.

The United Kingdom has managed to draw upon a wealth of experience in dealing with crowd and transport related disasters from the 1980s and 1990s, in thinking about the task of CIIP. These lessons taught that no one single agency has the ability and resources to respond effectively to a disaster involving CNI.[26] 11 September 2001 in the United States and 5 July 2005 in London, highlight the fact that 'conventional' terrorism still poses a significant risk for society and the government. But there have been other events, which demonstrate the emergence of a new threat (which was predicted some time ago as a possibility), with attacks on CII in the UK. To illustrate the level of the problem there was a news report stated that in 2005, "nearly 300 UK government departments and businesses critical to the country's infrastructure were the subject of Trojan horse attacks, many reportedly originating in the Far East."[27]

[25] CPNI website, http://www.cpni.gov.uk/aboutcpni188.aspx, accessed 3 September 2008

[26] *Critical Infrastructure Protection and Crisis Management in Britain*, IAAC Briefing Paper, No. 14, 8 January 2001

[27] *Fingers Pointed at Chinese Military After Hacking Reports*, Sophos, http://www.sophos.

The issue of CIIP and Defensive Information Warfare raised a heightened interest in 1994-95, but was debated in its early forms in the UK already by 1990. The developments are unfortunately not that publicly traceable as UK sorted these issues much to the domains of its intelligence community. NISCC was in reality a virtual coalition with a small staff of its own and technically dependent on the Central Electronic Security Group (CESG) – the information security branch of the UK signals intelligence agency GCHQ in Cheltenham.

Australia[28]

The definition of CI, according to the Australian concept is as "infrastructure which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on social, or economic well-being or affect national security or defence." There is an identified subset of CI, national information infrastructure (NII). This is defined as being "a subset of the critical infrastructure which comprises the electronic systems that underpin critical services such as telecommunications, transport and distribution, energy and utilities, and banking and finance." The aim of CIIP, according to the Prime Minister was "to assure Australians that both the physical safety of key assets as well as the information technology systems on which so many of them depend is protected." (Abele-Wiegert & Dunn, 2006, pp. 35-36)

Events that appear to have sparked an Australian interest in actively seeking to protect their Critical National Infrastructure occurred in the late 1990s. A Foreign Affairs, Defence and Trade Group research paper in 1998, drew attention to the issue. Dr Cobb of the Australian National University observed that; "while law enforcement organizations are concentrating on physical security they do not appear to have canvassed cyber-security issues." Awareness and perception of the potential risk was further elevated by the Sydney Olympic Games in 2000, which put the nation's reputation on the line in front of the world and simultaneously making Australia an attractive target.[29] It seems that the trigger for Australia to look into its information infrastructure security was the Olympic Games. There was a lot at stake in terms of national pride and political reputations.

Going back to 1997, the National Police Research Unit (NPRU) published the report, *Minimum Provisions for the Investigation of Computer Based Offences*. In November 1997, the report was endorsed by the Australasian Police Ministers' Council (APMC), and then referred to the Standing Committee of the Attorney General (SCAG) for consideration. A committee, which reports to SCAG, the Model Criminal Code Officers Committee (MCCOC) released

com/pressoffice/news/articles/2007/09/chinese-hack.html, 5 September 2007

[28] The main agency through which CIP is regulated in Australia is the Trusted Information Sharing Network, information can be found on their website - http://www.tisn.gov.au/

[29] IAAC Briefing Paper. 19 October 2000. *Australian and Canadian policy Overviews*, No. 11

Comment is from: Dr A. Cobb, Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks', www.aph.go.au/library/pubs/rp/1997-98/98rp18.htm, 19 September 2000 a report in January 2000 titled *Chapter 4: Damage and Computer Offences*. The proposals were very similar to the UK's 1990 Computer Misuse Act.[30]

Products and services that have been defined as being CI in Australia include; communications, energy, finance, food supply, government services, health, manufacturing, National Icons (such as Opera House), transport and utilities. (Dunn & Wiegert, 2004, pp. 39-40) These products and services are considered essential for Australian society to continue functioning in its current state of development.

The agency that bears much responsibility for CIP and CIIP is the Australian Security Intelligence Organization (ASIO).[31] They work with the Federal Police and Defence Signals Directorate in relation to threats affecting the National Information Infrastructure. It has developed the Protective Security and T4 programs. These programs are under the guidance of the Security Construction and Equipment Committee (interdepartmental), which reports to the Protective Security Policy Committee (an interdepartmental body that oversees protective security policy in Australia).[32]

In early 2003 it was publicly announced that a new inter-agency online security agency had been formed in order to protect Australia's information infrastructure against perceived threats such as; viruses, hackers and cyber-warfare. The new body, the *E-Security Coordination Group*, their tasks include; setting the standards for security reporting and skills; organizing responses to any attacks made on the national information infrastructure. The agency is operating under the National Office for the Information Economy. Threat and vulnerability assessment is to be conducted by a new sub-committee, the *Critical Infrastructure Priorities Group*, which is under the authority of the Attorney-General's Department.[33]

A key part of the CIP programme is the Trusted Information Sharing Network (TISN), and in particular an integral part of it, the Critical Infrastructure Advisory Council (CIAC). TISN was announced by the Australian PM in November 2002. CIAC provides advice to the Attorney-General's Department on a national approach to CIP. They are part of a wider network in North America, the Information Sharing and Analysis Centres (ISAC).[34]

[30] Australasian Centre for Policing Research. 2000. *The Virtual Horizon: Meeting Law Enforcement Challenges*, Scoping Paper, Payneham (Australia), pp. 96-7

[31] To find out more about the ASIO please refer to their website: http://www.asio.gov.au/ ASIO defines critical infrastructure as "those physical facilities, supply chains, information technologies and communications networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security". http://www.asio.gov.au/Work/Content/CIP.aspx

[32] IAAC Briefing Paper. 19 October 2000. *Australian and Canadian policy Overviews*, No. 11

[33] *Australia: Government Regroups in War Against Cyber-Crimes*, The Canberra Times, 1 February 2003

[34] *Report of the President of the United States on the Status of Federal Critical Infrastruc-*

Australia did start off quite late with the debate on information threats (1997-98) but had a very fast implementation phase due to the Olympics in 2000. The results of different interdepartmental committees in this area though are not that transparent as these not were public investigations.

Sweden

A number of committees were formed in the 1990s and in the early 2000s dealing with issues arising from a re-thinking and a revamp of the crisis management and civil emergency system. The Cabinet Working Group on Defensive Information Operations (Ag IO/IW) was established on 12 December 1996. Its members were drawn from the cabinet office and concerned agencies with the main task to produce a new strategy on these new digital threats, and it produced two reports in 1997 and in 1998. The latter suggested a new holistic Information Assurance scheme with changed organisational responsibilities, and which also became the basis of a Cabinet Bill in 1999 and a Parliamentary Decision the same year. The group did also visit Finland and Norway in 1997 and 1998 to brief on their reports.

In its later more consultative phase from 2000 the Working-Group also included members from pertinent private companies and organisations. Duties of this working group in this phase included; monitoring emerging threats and risks within the sphere of information warfare and to spread information about them; proposed solutions on assigning responsibilities and formulating guidelines in order to develop a strategy for guarding against IO. The group was disbanded at the end of 2002 when some of its functions was transferred to the newly established Swedish Emergency Management Agency (SEMA). (Christiansson & Fischer, 2005, p. 6) The main "customer" and promoter for Cabinet WG during this period was the parliamentary composed Defence Commission under its dynamic chairman Håkan Juholt (MP).

Other commissions and committees have followed. A Swedish government decision on 23 June 1999 authorised the Minister of Defence to lead a commission of inquiry that was designated the task of analysing and submitting proposals for standards that would generate a more integrated approach to civil defence and planning/preparation for emergencies. In May 2001 the Commission on Vulnerability and Security delivered its report, which was regarded as a significant step towards the intended changes. The report highlighted a lack of coherency in the system in Sweden for dealing with serious IT threats. One suggestion on how to help remedy this was the formation of an agency for Information Assurance (IA). During 1997-2003 there existed some six different committees on CIIP, somewhat parallel, all tasked with creating a national strategy.

The importance of CIIP in Sweden can be judged by the government bill *An Information Society for All* (1999/2000:86), which stated the desire that Sweden was to be come the first country in the world where information society was

ture Protection Activities, January 2001, p. 12

for all. (Christiansson & Fischer, 2005, p. 9) In 1972 Sweden was the first country to introduce a Data Protection Act (SDPA), which was reformed in 1998 to fit with EU standards, and renamed the Personal Data Act (PDA). This act regulates the handling of personal data in both electronic and non-electronic forms. (Christiansson & Fischer, 2005, p. 10) With a lot of functions between government, citizens and business done over the internet, plus the CII, Sweden has a number of vulnerabilities and serious consequences for the functioning of society if CII is inoperable.

This raises the question, which agency or agencies are responsible for the running and protection of CII in Sweden? There are a number of governmental agencies involved in CIIP, the primary ones are; SEMA, the Swedish Defence Material Administration (evaluating threats), Swedish National Defence Radio Establishment (locating the source of threats), and the Swedish National Post and Telecom Agency (security issues related to ICT). SEMA shall be the focus of this part of the article.

Established on 1 July 2002, SEMA took over some functions from its predecessor organisations (Swedish Agency for Civil Emergency Planning and the National Board for Psychological Defence). It is the coordinating body for civil preparation in times of crisis and war. Within SEMA is the Information Assurance Department, which educates, researches, develops and informs different stakeholders (in the state sector and the private sector) on issues relating to information assurance. It also manages the National Council of Information Assurance (successor to the Cabinet Office Working Group on Information Operations). (Christiansson & Fischer, 2005, pp. 14-15) In addition to the tasks of coordinating the above, SEMA encourages interaction between the public and private sectors and has a number of collaborations with similar agencies overseas.[35]

Sweden was a relatively early starter in the process of CIIP. Their initiation of the process also sparked other Nordic countries (such as Finland and Norway) into starting their national CIIP programmes too. However, the political system that does not allow for a strong central leadership, combined with the nature of the state bureaucratic structures meant that progress has slowed considerably as the result of increased resistance and friction among the various actors in the process.

Finland

The issue of CIIP in Finland has received a high priority, and being vital to the national interest. Security measures undertaken in Finland are based upon the *Security of Supply Act* and on the order of the *National Emergency Supply Agency* (NESA), which was established in 1992.[36] (Dunn & Wiegert, 2004, p.

[35] Harrop, M. 2003. *Approaches to Critical Network Infrastructure Protection: An Overview of Measures Being Taken by Some Countries Outside North America to Protect Critical Network Infrastructures*, Canada, Electronic Commerce Branch, Industry Canada, Contract 5009657

[36] Another significant document from the 1990s was released by the Ministry of Finance

75) Throughout the 1990s there were a number of reports published on the theme of information society.

A report named *National Outline Policy for the Development of Information Networks 1995-1998*, which was produced by the Ministry of Transport and Communications. The purpose of the report was to investigate methods for enhancing the infrastructure for data exchange. Reports such as this formed the basis for departments to produce action plans and to make funds available for projects concerning information society. A *National Information Society Committee* and an *Information Society Forum* were created by the Ministry of Finance in 1997, and with some obvious influences from the first Swedish report the same year. The Ministry of Transport and Communications concentrated upon the technical and security related aspects.[37] (Dunn & Wiegert, 2004, p. 76)

In 2000, the *Information Society Advisory Council* (Ministry of Finance), published the report *Finland as an Information Society*. It summed up the then current situation in terms of the stage of development, and attempted to gauge the economic and social effects of information society. Other topics that were dealt with included the promotion and development of information society, and the domestic regulatory framework for it. (Dunn & Wiegert, 2004, pp. 76-77) The first step, as has been the case in a number of other country approaches, was to consider what Finland already had in terms of CII, and then to evaluate its level of importance to Finland (i.e. understand the effects should the CII cease to function).

In June 2001 the Ministry of Defence handed in a report, *Finish Security and Defence Policy 2001*, to the parliament. One of the cornerstones of the document was the broadening of the concept of national defence, to include; military, economic, civil defence, social welfare and healthcare, technical systems operation, public order and security, and defence information activities. The body that is responsible for defining the areas and sectors that are vital to society is the *Security and Defence Committee*. It is in charge of drafting a national strategy for precautionary measures. According to the report:

> The precautionary measures cover both military and civilian measures […] and are based on extensive cooperation as the activities in different sectors of society become more interdependent. (Dunn & Wiegert, 2004, p. 77)

These developments demonstrate an awareness that measures cannot be taken piecemeal as the different sectors are interconnected and therefore vulnerabilities in one part of the system weaken the system as a whole, and the boundaries between civil and military also begin to fade in this regard.

A contact point for citizens, government, business and organisations was set up by the government, the *Advisory Committee for Information Security* (ACIS),

in 1997 on *Data Security and Law*. An executive summary of this is available in English.

[37] Also see www.oecd.org/dataoecd/18/5/2004573.pdf *for more information on general CIIP policies in Finland.*

was established as a focal point regarding information security issues. ACIS is subordinated to the Finnish Communications Regulatory Authority (FICORA), and reports to the Council of State. It provides a forum for different sectors of society in the management of information security concerns.

The first stage of ACIS work involved the publication of the report *Information Security Review* in June 2002. This was a summary of security threats that could potentially affect Finland, and a number of suggested measures to counter them. The stated goal was that "Finland will be an information-secure society that everyone can trust and that enables all parties to manage and communicate information safely." November 2002 saw the release of the *National Information Security Strategy Proposal* by ACIS, which was accepted by the government on 4 September 2003. In this document there was a focus on policy objectives (and how they were to be met), contingency planning and the assignment of responsibility to the various stakeholders that are involved. (Dunn & Wiegert, 2004, pp. 78-79)

In 2003, the Finnish government issued a paper, *Strategy for Securing the Functions Vital to Society*, which divided vital functions into seven areas: state leadership, external capacity to act, national military defence, internal security, economy and society, population's livelihood and capacity to act, and mental crisis endurance. It is a follow-up on the preceding papers, with updated versions appearing in 2006 and the next in 2010. In addition to the regular reports, the Security and Defence Policy report is submitted by the government every three to four years to the parliament. (Abele-Wiegert & Dunn, 2006, p. 86)

Finland's approach to CIIP is very systematic and comprehensive. The process began with understanding the nature of sector; moving to identifying possible threats and the consequences; then progressing to suggesting remedies and assigning responsibilities to various actors. The time-span is reasonably prompt, which implies that there is a perception from the authorities that this is a potentially serious problem, this is then transformed into political will to resolve the highlighted problems.

We find here that Finland came out quite early (1997) with government initiatives just after the issue been raised, but the process was somewhat halted when it came to formulate a coherent government decision. The implementation phase after the decision was made seem though to have a very good momentum.

Norway

From the late 1990s the issue of CIIP has received greater attention and importance in Norway. This began with the *State Secretary Committee for IT* (SSIT) in 1998, which formed a sub-committee with the intention to survey the state of IT vulnerability. The *Defence Review 2000* and the *Defence Policy Commission 2000*, both also stressed the importance of CIIP. Then the events of 11 September 2001 pushed the issue of security to the top of the political agenda, as it did in most other parts of the world too. (Dunn & Wiegert, 2004, p. 150)

These various policy statements set the background for the events that set the reasoning and the agenda for CIIP. The process was prompted, perhaps in part, due to Sweden's work in the area that began in the late 1990s.

A number of decrees, commissions and projects were also initiated during the period from the 1990s until the early 2000s. Findings from the governmental commission on *A Vulnerable Society*, which was established by royal decree on 3 September 1999, provided a stepping stone in the process of establishing priorities and policies. One of the controversial recommendations of this commission was that safety, security and emergency planning should be handled by a single ministry. It also proposed the following: a partnership between the public and private sector, promote information exchange, create early warning capacity, harmonisation and adjustments of laws and regulations, public responsibility for CIP is vital to ICT systems. (Dunn & Wiegert, 2004, p. 151) The commission laid the groundwork for determining future priorities and how the goals were to be achieved.

The Ministry of Trade and Industry was responsible for setting in motion a number of initiatives concerned with the vulnerability and security of ICT in Norway. This began in 1999 with the *ICT Vulnerability Project*. This group coordinated with the *A Vulnerable Society* group to present their findings. This culminated in the *National Strategy for ICT Security*. The national strategy was published in June 2003, which proposed a number of ideas along the lines of the *OECD Guidelines for the Security of Information Systems and Networks*. The concept of security, which ranged from the individual through to the national level, which related to the use and functioning of ICT. The strategy began to be implemented from the autumn of 2003, beginning with the opening of the *Centre for Information Security*, and other initiatives such as education and awareness programmes. (Dunn & Wiegert, 2004, p. 152)

In the spring of 2002, two more initiatives commenced, on 5 April 2002 the Ministry of Justice and Police issued report No. 17 on the *Safety and Security of Society*. This was a report that focussed on the issue of the consequences should the failure of CI occur. A result was the formation of the *Directorate for Civil Protection and Emergency Planning*. The second event, worthy of mention is the presentation of the *eNorway 2005 Action Plan* in May 2002. It describes the needs, responsibilities and action that are required to develop IT society. This is linked with the European Union *eEurope Plan*. A focus was made on e-Government and e-Business. (Dunn & Wiegert, 2004, pp. 152-53)

Norway's initiatives seem to be sparked or at least guided by initiatives that are occurring in neighbouring environment. But once sparked, they are very quick in implementing the initiatives.

Norway was a late starter (1998) but geared up with the creation of the governmental commission under the former Prime Minister Kåre Willoch. There also seems to have been significant influences from Sweden's second report of the Cabinet Working-Group on organizational structures.

Explaining Differences and Similarities

If we based on the country descriptions above try to identify and extract by year the five phases/milestones we want to look at the following table will appear.

Comparative Country Approach

Country	EW/ Debate	Decision on Investigation/ Enquiry	Proposals from Investigation	Cabinet Bill/ Parliamentary Decision	Implementation
USA	1993-4	1995 (*PCCIP)	1997 (PCCIP)	1998 (PDD63)	1998
UK	1990	1996	1999	2001	2002
AUS	1997-98			1999	1999
SWE	1994-6	1996	1998	1999 (2000)	2003
NOR	1997	1998 + 1999	2000	2001	2002
FIN	1997	1997	2001	2002	2003

*PCCIP – Presidential Commission of Critical Infrastructure Protection

From observing the timelines of the individual countries in the above table, a number of quick points can be made for each of the countries listed.

The United States seems to have the shortest decision-making cycle of the studied countries (with a *OODA-Loop* in military jargon) from the Early Warning to the Implementation phase. In one sense, this is somewhat of a paradox as it is often stated that the United States has one of the biggest (and hence implied cumbersome) bureaucracies in the world. On the other hand, it may not be that strange as this is where the debate on CIIP began. Another factor that may have had an effect is the US Constitution and its 'spoil-system', which promotes fast results as it is tied to the four year presidential term.

A problem arose in the case of the United Kingdom, which was that the process was rather hard to trace. This appears to be the result of the constitutional system, which is not very transparent, in terms of public investigations etc., as other Western democratic states. Often the administrative development takes place within ministerial and Cabinet Office committees. One reason for this could also be that UK - in contrast to the other countries in this survey - to a large extent put these issues into the "intelligence portfolio", where the British Security Service (MI 5) has got a key role.

Australia experienced a late detection phase, however, the implementation phase was attained very quickly. This should been seen within the context of the situation, which demanded a sense of urgency. With the Olympic Games (and Y2K) due to be held in Sydney in 2000, an overhaul of all government protective schemes and programmes was undertaken. Australia is also a relatively homogenous country, which is reflected in its administrative system, which has the effect of hastening the decision-making process.

Sweden detected the problem quite early and enjoyed a good momentum early on in the process, up until the implementation phase when things seemed to grind to a halt (1999-2003). A possible explanation for this is the odd Swedish Constitution (in European terms), with its small cabinet departments and big independent agencies. Added with the fact that 'ministerial rule' is explicitly forbidden. Such a system demands a strong 'judge' (i.e. a strong Prime Minister's Office) to resolve conflicts that emerge between different sectors in the form of 'turf' fights between agencies on cross-sector issues, which often continues up to their respective Cabinet Departments. An absence of a strong 'judge' could explain the halt at the implementation phase.

Although Finland entered the process rather late, fast results have been achieved, with the Ministry of Finance taking the lead. However, work does not in the early phases seem to have been coordinated with the Ministry of Defence or Interior, which may account for a pause in the process. It all seems to have been put back on track again when the Defence and Security Committee received a wider mandate that encompassed CIIP.

Norway in comparison, detected the problem somewhat later, but implemented the CIIP programme much quicker than Sweden. The Norwegian system is characterized by a strong system of ministerial rule, which seems to lead to a faster implementation phase after two or more ministers are able to come to an agreement.

Another way of clustering the diffusion of ideas is that USA, UK and Australia (together with Canada and New Zealand) are part of the "five-eyes club" with strong multi- and bilateral intelligence relations. This leads also to more of information sharing on threats and a common view on how to protect their common inter-dependable information networks.

The various policies on how to protect the wider information society – for example between the USA and the UK - seems though to be based on the different constitutions and different approaches to the role of the intelligence community in their national Information Assurance schemes. USA treated the CIIP as new "operational" political issue and created new institutions with some support of the intelligence community, while UK to a large extent treated this as an intelligence and security matter coordinated within Whitehall and with some new responsibilities given to existing organisations.

A second possible clustering here is the Nordic countries where Sweden adapted the US debate early and where ideas influenced the processes in Finland and Norway, even if the constitutional framing differed.

These reasons may perhaps explain why Norway was able to pass through the process of initiating the debate through to implementing the decisions. It has a cash surplus due to the oil reserves, this being coupled with perception of threat and the realisation of the consequences should CII be attacked. Most important though was that it put its intelligence community as the lead body during the initial phases and thus bridged the traditional gap between the Intelligence Services and Law Enforcement bodies. Some bureaucratic turf fight did appear later though when the protective measures should be implemented within other parts of government, as the intelligence community generally doesn't have the budget to handle these problems.

In a number of cases, the trigger for initiating the process of CIIP policy was the result of another country beginning the process. Either way, it had the effect of 'kick-starting' the process through raising awareness and creating perception of the issue and prompted governments to act on an issue (by raising the priority of the issue).

A number of the countries studied have failed to implement policy, even after a quick and determined start to the process. There appear to be a number of reasons for this failure. One possible reason being, as mentioned above, the issue of scarcity of resources for the state. This problem being compounded by the fact that many of the CII resources are in the hands of the private sector, which complicates issues of jurisdiction and who foots the cost. Another possible reason for the apparent loss of drive is a possible lowered level of threat perception by a number of countries. This being the result of no more major terrorist attacks on the scale of 9/11 and perhaps a feeling of being 'safe' as they do not perceive themselves as being an attractive target (when compared to the United States for example).

Conclusion

The issue of CIIP initially began as a military issue, but soon came to encompass the whole spectrum of society. An initial event triggered the debate and early warning phase in some of the cases, whether the event affected the country in question or an event abroad was responsible. In some cases it was the events of 9/11 in the United States, for others it was the approach of Y2K, and for Australia it was the approach of the Olympic Games in Sydney. The United States was in the lead with regard to recognising the potential of the problem.

A factor that exacerbates and compounds the potential for a serious incident is the fact that many of those vital systems are taken for granted. The development of automated control systems that regulate our everyday lives (such as air traffic control, provision of electricity and water) has increased the standard of living and prosperity, but it has simultaneously introduced new threats and vulnerabilities. Such a situation (in terms of threat) requires a coordinated approach to try and resolve. The United States is in the position of being a super-power and therefore likely to be challenged by a range of potential threats that seek to expose weaknesses. Other countries, such as Finland, have a lot of political and economic capital tied up in the IT sphere. If this is harmed profits are endangered and political careers are put in jeopardy.

A country's ability to successfully navigate the various identified phases of the CIIP programme implementation process is determined by a number of observable factors. One of these is the nature of the constitutional structure as it relates to the state bureaucracy. The United Kingdom has a tendency to use committees behind closed doors. Ministerial rule which is applied in Norway, when compared to Sweden, seems to hasten the process, especially when combined with a clear set of goals and using another country's experience (Sweden) to boost the process. These cases would appear to demonstrate the need for an effective top down management of the process in order to stop it from being delayed or stalling.

There has also been a tendency to try and concentrate the responsibilities for CIIP into as fewer different ministries and departments as possible. The United Kingdom has done this recently; Australia has employed this tactic too. Sweden on the other hand, involved a number of different agencies in the same task, and also lacked the strong top down management of the process. Consequently the time span of the implementation process was long.

These findings tend to point to an observation made by Peters; Change can be brought about by a number of different factors that exist in the institutional environment. This may be the result of a perceived current need, which should be addressed or could be the result of an anticipated need. Bureaucratic institutions are prompted to change by their environment, the example of legislatures have been used to demonstrate the point.

> Legislatures in most countries have become professional and more institutionalised, often as a means of counter-acting the increasing powers of political executives. This implies that in this perspective institutions change in response more to external stimuli than to their own internal values, although statements of that sort are rarely discussed. [38] (Peters, 2005, p. 100)

A possible explanation for the delays found in the policy implementation process is taken up Kingdon. This becomes especially relevant when a number of agencies are involved in the road to shaping and enacting policy. A problem highlighted by Kingdon in the process towards administrative reform are the political interest and compromises that take place among the different actors in order to come to some agreement. He also points out a number of factors that may motivate some actors, not previously involved in the process, to become involved. In turn, this affects the general perception of the situation.

> Consensus building in the political arena, in contrast to consensus building among policy specialists, takes place through a bargaining process rather than by persuasion. Once participants sense that there is some movement, they leap in to protect their interests. This entry into the game, sometimes sudden entry, contributes to a sharp agenda change, both because various interests receive some benefit from their participation, and because a generalised image of movement is created. (Kingdon, 2003, p. 163)

This has the potential to affect the entirety of the process, from the realisation of a potential problem to enacting policy that has been passed through

[38] Peters (2005) states that research into the area of institutional change is not well developed. (p. 61)

parliament. Therefore it is critical to understand, and to foresee these types of problems. It cannot be stressed enough, these processes and phenomena require more research in order to draw more decisive results. This article is but a very modest step in that direction, and it is hoped to spur more research in this direction.

From the current theoretical standpoint, it is often assumed that political actors are rational and behave in a predictable manner in order to achieve the desired outcome. This does not take into account a whole range of complexities and interests that can have the potential to alter this theoretical ideal. Among other things, this article points to the potential effects that issues such as perception among the actors, and the issue of competition for resources and prestige. There is also a hint that these aspects are often overlooked or mismanaged in the policy change process, which results in lengthy delays or the complete stalling of progress. Once more, it needs to be said, this needs further empirical investigation in order to start illuminating some clearly definable and defendable trends.

One preliminary thesis that without greater risk then could be used – also based on the observations and findings in this article - would be that though the political system controls the decision-making process (i.e. the first four milestones in this article) within the central government machinery, they exercise far less control over the implementation.

References

Abele-Wigert, I. & Dunn, M. (Wenger, A. & Mauer, V. Series editors) 2006. *International CIIP Handbook 2006: An Inventory of 20 National and Six International Critical Information Infrastructure Protection Policies*, Vol. 1, Zurich, Centre for Security Studies (ETH)

Allison, G. T. 1971. *Essence of Decision: Explaining the Cuban Missile Crisis*, New York, Harper Collins Publishers

Armistead, L., ed., 2004. *Information Operations: Warfare and the Hard Reality of Soft Power*, Washington D. C., Brassey's Inc

Collin, B. C. 1996. *The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge*, proceedings of the 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago

IAAC Briefing Paper. 8 January 2001. *Critical Infrastructure Protection and Crisis Management in Britain*, No. 14, http://www.iaac.org.uk/

CSIS Task Force Report (Global Organised Crime Project). 1998. *Cyber-crime … Cyber-terrorism …Cyber-warfare: Averting an Electronic Waterloo*, Washington D. C., CSIS Press

Dunn, M. & Wigert, I. (edited by Wenger, A. & Metzger, J.) 2004. *An Inventory and Analysis of Protection Policies in Fourteen Countries: Critical Information Infrastructure Protection*, Zurich, Centre for Security Studies (ETH)

Dunn, M. & Mauer, V., eds., 2006. (Wenger, A. & Mauer, V. Series editors), *International CIIP Handbook 2006: Analysing Issues, Challenges, and Prospects*, Vol. 2, Zurich, Centre for Security Studies (ETH)

Kingdon, J. W. 2003. *Agendas, Alternatives, and Public Policies*, 2nd Edition, New York, Longman

Libicki, M. C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*, New York, Cambridge University Press

Lukasik, S. J., Goodman, S. E. & Longhurst, D. W. 2003. *Protecting Critical Infrastructure Against Cyber-Attack*, New York, International Institute for Strategic Studies, Adelphi Paper 359

Molander, R. C., Riddile, A. S. & Wilson, P. A. 1996. *Strategic Information Warfare: A New Face of War*, Santa Monica, National Defence Research Institute, RAND

Peters, B. G. 2005. *Institutional Theory in Political Science: The 'New Institutionalism'*, 2nd edition, London, Continuum

Article 2

Understanding Intelligence Community Innovation in the Post-9/11 World

Published 2011 in
International Journal of Intelligence and Counterintelligence
(Vol. 24, No. 3, May 2011, 534-568)
by Routledge

Abstract

The purpose of this article is looking towards at how Intelligence Communities innovate (adaptability) and how the new demands of pluralism in the intelligence production process have been fostered. By innovation, it is specifically meant that intelligence organisations and the legal/political machinery in the sector evolve to meet the changes and challenges found in their environment.

1. Introduction

This article demonstrates that there has been significant investment in and transformation of the United States Intelligence Community (IC) in the wake of 9/11. But where is all of this growth and investment heading? The matter dealt with on the macro-level is on one side the level of reactive adaptability to *change* when an institution(s) is confronted by new forms of external threats and obvious failures. The other side is how to proactively and in a controlled fashion promote pluralism and *innovation* in order to create an agile and successful organisation able to continuously adapt the business processes to the developments of society and targets.

A subtle, yet importance difference lies in the distinction between c*hange* and i*nnovation*, for the purposes of the article. *Change* is most often something that is imposed upon an organisation, especially in the wake of an obvious failure. On the other hand, *innovation* is a process of 'fine-tuning' the system in order to meet evolving or anticipated challenges, and can be internally driven. This article is about change and innovation in the intelligence system as a whole in the United States, but is equally applicable to the system at the organisational level. A particular focus is on the dynamics *within* each stovepipe - *not between* as there has not a good record of results from change and innovation undertaken to date. An article in July 2010 in the Washington Post highlighted a number of these problems.[39]

There is a deliberate distinction where there is a change of equilibrium between agencies as opposed to change within an agency. According to Andrew Van de Ven in *Central Problems in the Management of Innovation*, he defines *innovation* as being "the development and implementation of new ideas by people who over time engage in transactions with others within an institutional order."[40]

Why is this of interest then? Within the area of Public Administration and Public Management very little has been written on how the IC as traditionally rigid organisations in the core of the State Apparatus evolve and adapt to new

[39] Dana Priest & William Arkin, *A Hidden World Growing Beyond Control*, Washington Post, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/, 19 July 2010

[40] Andrew Van De Ven, *Central Problems in the Management of Innovation*, Management Science, Vol. 32, No. 5, May 1986, p. 590

circumstances when there are no market or other competitive mechanisms present. One of the dilemmas that are presented in the current age of reforming governmental structures is trying to understand the nature of government. A simple and yet tough question needs to be asked "is government a business"? The answer to which, and the application of the findings in terms of the nature of the proposed reforms, may have a profound effect upon structures in the intelligence community.

It is acknowledged that *innovation* can be squashed in 'closed' organisational systems. The United States' management system of a top-down command structure and the compartmentalised physical organisation of the parts of an organisation tend to stymie the fostering of an innovative culture.[41] Whilst understanding and acknowledging that this does occur, the focus of this article is not upon this type of system. Organisational learning feeds into the theory on innovation and helps us to understand some of the aspects that not only help innovation and change, but also either hinder or block it.

An underlying assumption here is that the US Intelligence machinery is a driving force compared to for example European Intelligence Communities – although in this article the United Kingdom is mostly used to illuminate the dichotomy - they seem to be more conservative and to adapt more slowly. In this article I will try to examine if this postulate can be supported theoretically by the general approaches to innovation and developments within these communities. From a comparative perspective, the primary research question is whether the 'young' US IC more innovative than the 'old' European ICs or are there other factors like resources and technology that play a more significant role?

There have been a remarkable number of changes since the end of the Cold War in 1991. A number of academics saw an end to conflict with the end of the bipolarity that marked the Cold War period (as exemplified by Francis Fukuyama and the End of History). However, what this new era heralded in was a new set of challenges and risks. These were not based on the principles of the Cold War, although in some ways it is possible to argue they were linked. Instead of having state actors, which are generally assumed to act in a rational and predictable manner, the new opposition is non-state based. The new adversary, which now begins to fall under the general rubric of al-Qaeda, is based on an extreme version of Islam and is committed to a long, uncompromising and bloody asymmetric struggle.

[41] Rod Hague & Martin Harrop, *Comparative Government and Politics*, 7th Edition, Basingstoke, Palgrave MacMillan, 2007, pp. 361-2

2. Theory of Innovation

Framing

The way that this article is framed and focused needs to be explained as the issue of the subject of innovation within the IC is very broad and involves many different levels. Therefore, this article does not focus on relations between the producer (IC) and the consumer/policy maker, which is the focus of the likes of Sherman Kent. The horizontal relation between different agencies is also not the focus. What is the focus of this work is the internal and intra-agency process.

There are a number of other associated points that need to be clarified before proceeding further, in order to specifically identify the exact subjects and objects of interest. A distinction needs to be drawn at this stage between "change" and "innovation". Innovation within the IC forms the subject of interest. This process is often an internally driven one, designed to address identified or presumed changing needs or deficiencies within the existing system.

Intelligence activity can be carried out either on a reactive or proactive basis. There are attempts to try and think ahead and understand what is going to happen in the future and try to adapt to those assumptions, such as the Cold War era intelligence assessments of the Soviet's military capacity, at times forecasting decades out. A problem with proactive intelligence is that it connects more with current political requirements, which makes it more problematic to analyse. For this reason, this work will mainly be looking at *reactive* intelligence.

A final consideration within the frame of this article is that there is a focus on the stated problems from a public management perspective. To be even more specific, public management concerning government organisations at a macro-level, and without any competitive market/economy incentives that would influence the outcome.

Theoretical considerations

New Public Management (NPM) is a policy 'creed' that has been adopted by the Anglo-American world of public administration since the end of the last century. It has led to radical change to the public sectors of the countries that constitute the Anglo-American world (Australia, Canada, United Kingdom and especially New Zealand). One of the inspirations of NPM is summed up by one of President Reagan's comments: "government is not the solution to the problem; government is the problem."[42]

An approach to understanding NPM is helped by considering Osborne and Gaebler's *Reinventing Government* article from 1992. It enumerated 10 principles for improving the effectiveness of government agencies.

1. Promote competition between service providers;

[42] Rod Hague & Martin Harrop, *op. cit.*, p. 366

2. Empower citizens by pushing control out of the bureaucracy into the community;
3. Measure performance, focusing not on inputs but on outcomes;
4. Be driven by goals, not rules and regulations;
5. Redefine clients as customers and offer them choices – between schools, between training and programmes, between housing options;
6. Earn money rather than simply spend it;
7. Prevent problems before they emerge, rather than offering services afterwards;
8. Decentralise authority and embrace participatory management;
9. Prefer market mechanisms to bureaucratic ones;
10. Catalyse all sectors - public, private and voluntary – into solving community problems.[43]

Hague and Harrop also identify a number of components and characteristics associated with the practice of NPM. These include: managers are given more discretion but held more responsible for results; performance assessed against explicit targets; resources allocated according to results; departments unbundled into more independent operating units; more work contracted out to the private sector; more flexibility allowed in recruiting and retaining staff; costs cut in an effort to achieve more with less.[44] NPM takes a more business-like approach to the issue of transforming the public sector from a bureaucracy into a responsive and flexible organisation.

Metcalfe (1993) argues that there is a need for new theoretical foundations if public management was to be able to make the transition from imitation to innovation. He characterised governmental approaches to management problems in the 1990s as being mere imitation of business management practices, and that it was time to move beyond this, and towards innovation. Innovation he states, entails the "development of new methods of management appropriate to the distinctive needs of government."[45]

In his opinion there exist two major challenges facing contemporary governments within the sphere of public management. The first challenge is the fast pace and type of change that is being faced. Secondly, is that unlike business, governments operate through networks of interdependent organisations as opposed to independent organisations (that are simply pursuing their own objectives). In terms of the focus of public administration and public man-

[43] From David Osborne & Ted Gaebler, *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*, New York and London, Penguin, 1992 in Rod Hague & Martin Harrop, *Comparative Government and Politics*, 7th Edition, Basingstoke, Palgrave MacMillan, 2007, p. 367

[44] Rod Hague & Martin Harrop, *op. cit.*, p. 368

[45] Les Metcalfe, *Public Management: From Imitation to Innovation*, Australian Journal of Public Administration, Volume 52 Issue 3, Pages 292 – 304, 1993, p. 292

agement, Metcalfe sees that there has been a shift in emphasis and focus from stability to change.[46] This shift in governmental focus should mean a greater chance that some form of change in public policy problems in the contemporary setting than in the past.

In regard to the notion of innovation the article by Van De Ven (1986) is particularly useful to understand what is involved within a theoretical framework. According to Van De Ven, four basic concepts are critical to studying the innovation process: 1) ideas, 2) people, 3) transactions and 4) context. Van De Ven talks of the "currency of ideas" insofar as some ideas gain greater value and others are discounted for one reason or another. Innovation is shaped and guided to an extent by the frames and perceptions that the problem is viewed.

In July 2007 Christian Stadler had his article, *Four Principles of Enduring Success*, published in the Harvard Business Review.[47] The study by Stadler and a team at Innsbruck University's Business School compared nine pairs of European companies over 50 years. Four main findings were derived from the project, which Stadler refers to as being the four principles of success. These are:

1. "Exploit before you explore – great companies don't innovate their way to growth, but grow by efficiently exploiting the fullest potential of innovations that already exist.
2. Diversify your business portfolio – good companies, conscious of the dangers of irrational conglomeration, tend to stick to their knitting. But the great companies know when to diversify, and they remain resilient by maintaining a wide range of suppliers and a broad base of customers.
3. Remember your mistakes – good companies tell stories of success, but great companies also tell stories of past failures to avoid repeating them.
4. Be conservative about change – great companies very seldom make radical changes, and take great care in their planning and implementation."[48]

These particular principles were derived from the European business environment. However, they are equally applicable to innovation and change issues within the IC environment, especially in an era where government is being viewed and run as a business as governments face budgetary considerations and constraints and seek to streamline their operations. An "integrative challenge of building inter-organisational cooperation in the midst of structural change" is needed, according to Metcalfe. He also concludes that given the expansion of the role of management in government, it should be possible to employ existing business management practices more or less directly.[49] In a blog posting, Tony Campbell notes:

> In other words, at least two of the success factors recommend that there

[46] *Ibid.*

[47] Christian Stadler, Four Principles of Enduring Success, Harvard Business Review, http://harvardbusiness.org, 1 July 2007

[48] *Ibid.*

[49] Les Metcalfe, *op. cit.*, p. 303

> be caution about change. This is something to think about especially when intelligence managers are contemplating the "next" organizational change initiative. However, having said that, I would go back to the distinction between change that hits you and to which you have no choice but to manage adaptation for survival (responsive), and change that you have choice about launching or not and in what measure (proactive). What Stadler's advice underlines is that you better be very sure that the inevitable dislocations and costs of any change will justify the anticipated benefits. [50]

Principles one, three and four are the most applicable to the IC sphere, especially in the innovation and transformation aspects. In terms of innovation, do intelligence organisations seek to get the best from what they currently have or do they seek to embark upon something completely different? The third principle more relates to the subject of change, which is learning and admitting past errors and mistakes. The fourth principle should be highly relevant given the sensitive nature of intelligence and the risks involved in making major changes to intelligence agencies and the IC.

Another set of theoretical questions on the public policy process need to be asked, in order to place innovation within the context of change within the intelligence community in the public sector. It is useful here to get the perspective of former practitioners, formerly part of the IC, to appreciate where theory and practice intersect. Sims and Gerber offer their view of what they refer to as being 'true intelligence transformation' and what needs to be done in order to achieve this objective.

> True intelligence transformation fuses wit, creative business practices, and selected technologies for the purpose of achieving strategic advantage. It implies reform – the ability to beat adversaries faster, more efficiently, and with less cost to civil liberties than might otherwise be possible. But its trademark is the marriage of selected technologies with innovative strategies and practices such that revolutionary capabilities emerge.[51]

The notion of 'transformation' that is used by Sims and Gerber contrasts with this article's concept of innovation and change. In the quote, the nuts and bolts the process of *transformation* is enumerated without distinguishing between externally and internally controlled forces. In contrast this article makes a distinction between innovation and change, which is innovation from an internally driven perspective and change being an externally imposed process. Quiggin states his vision on the future of national security intelligence.

[50] Received via email from Tony Campbell on 13 September 2009
From 1993 to 2000, Campbell was responsible for foreign intelligence analysis in the Privy Council Office (Canada's Cabinet Office) as the Executive Director of the Intelligence Assessment Secretariat and Chairman of the interdepartmental Intelligence Assessment Committee. In 2001 he retired from government service. In 2006 he was made an Honorary Life member of the Canadian Association for Security and Intelligence Studies. His company, Campbell Intel Services is located in Ottawa, Canada.

[51] Jennifer Sims & Burton Gerber (Editors), *Transforming U.S. Intelligence*, Georgetown University Press; 1st edition, 2005, p. 10

> The role of national security intelligence will be broader and tougher in the future. Change will have to occur repeatedly and the agencies will have to reach out beyond their organisations to get the knowledge they need to meet the challenges.[52]

Here Quiggin sees the challenge for the IC in the future. On the one hand, the role of the state is in many cases diminishing in society and the role of the IC needs to reflect this change. On the other hand, risks and threats are diversifying and society is becoming increasingly vulnerable in a number of aspects (not least of which is technological dependency).

Lowenthal cites Richard Best on the reasons why reform and innovation is undertaken, which is divided into three broad chronological categories. 1) Within the context of the Cold War – to increase the efficiency of the IC. 2) As a counter to any criticisms as a result of failures of impropriety – Bay of Pigs, Iran-Contra deal, etc. 3) Post-Cold War era – refocus IC structure and requirements.[53] This implies the changing nature of the security environment necessitates changes in the state's early warning systems designed to detect sources of risk and threat.

The role of innovation in the US today can be seen in the National Intelligence Strategy (NIS) from August 2009 and which reveal a number of interesting aspects about the proposed priorities of the US IC.[54] It becomes clear that there is a clear focus of the 2009 NIS on one part of the intelligence mission; safeguarding national security interests from various threats. The other primary task is supplying foreign policy customers and maintaining information superiority (through information gathered and analysed for policy support and coordination.

The underlying reason for the NIS in the first place, is that it is a mechanism used to coordinate the activities (and accountability) of the 16 US intelligence agencies. Each NIS envisages a four year plan. The DNI stated the motivations and reasoning in a press release.

> This strategy advances our original, founding directive to achieve an IC that is integrated and collaborative. But it really goes much further than that. It reflects a more refined understanding of the threats we face and how we'll combat them. In describing our objectives, it prescribes methods for achieving them that can only be carried out by the IC that is agile, adaptive, and united. Most importantly, it recognises that national security hinges on good intelligence and it provides me with the tools that I need to monitor performance and ensure accountability.[55]

[52] Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age*, World Scientific Publishing Company, 2007, p. 22

[53] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 4th Edition, Washington D.C., CQ Press, 2009, p. 297

[54] *The National Intelligence Strategy of the United States of America*, Washington DC, The Office of the Director of National Intelligence, August 2009

[55] DNI Unveils 2009 National Intelligence Strategy, ODNI News Release No. 29-09, Office of the Director of National Intelligence, Washington DC, 15 September 2009

Organisational Learning

Learning is a central piece to understanding the issues involved in change versus innovation. It is entirely feasible for change and innovation can take place without learning. The important point to consider at this stage is not just that innovation takes place but that it promotes better intelligence analysis through improving the structure and processes employed within the IC.

Lovell does not differentiate between individual and organisational learning. He states that the elements are characterised "by primary reference to the intelligence and sophistication of thought which informs decisions, policies, and programmes, and to external efficacy, and by secondary reference to speed, completeness of relevant knowledge scan, and efficiency of thought and actions."[56] The process of organisational learning can be, to an extent, regarded as a process that is driven by perception.

Organisations are not actually capable of learning literally; rather this is a metaphoric term that is used to describe the process of "detecting" and then "correcting" an "error". The 'memory' of an organisation is derived from employees who act to adapt the "theory-in-use" of an organisation that are a reflection of an organisation's past experience. Therefore there can be no organisational learning without individual learning, however, although individual learning is a condition for organisational learning it is insufficient to bring about learning by itself.[57]

The application of organisational learning is the result of a process that involves negotiation and bargaining. This means that there is the influence of organisational and political dynamics upon the final result, and not the result of 'pure' logic, reason and analysis from previous experience.[58] As such, organisational priorities and politics can exert an influence on the process, resulting in the final product being less than an optimal solution for the identified problem, error or obstacle.

A lesson from the Second World War is useful in the delineation of organisational responsibility and ownership of tasks and functions. This was seen in the approach to the distribution of ownership and responsibility by the various belligerents involved in the conflict. Nazi Germany for example, saw the users

[56] John Lovell, "'Lessons' of Military Involvements: Preliminary Conceptualization," in Donald Sylvan and Steve Chan (eds.), *Foreign Policy Decision Making: Perception, Cognition, and Artificial Intelligence*, New York, Praeger, 1984, pp. 129-157, p. 133

[57] (1) Argyris and Schön quoted by John Lovell, "'Lessons' of Military Involvements: Preliminary Conceptualization," in Donald Sylvan and Steve Chan (eds.), *Foreign Policy Decision Making: Perception, Cognition, and Artificial Intelligence*, New York, Praeger, 1984, pp. 129-157, p. 133

(2) Bo Hedberg, "How Organizations Learn and Unlearn," in Paul Nystrom and William Starbuck (eds.), *The Handbook of Organizational Design*, New York, Oxford University Press, volume 1, 1981, pp. 3-27, p. 3

[58] John Lovell, "'Lessons' of Military Involvements: Preliminary Conceptualization," in Donald Sylvan and Steve Chan (eds.), *Foreign Policy Decision Making: Perception, Cognition, and Artificial Intelligence*, New York, Praeger, 1984, pp. 129-157, p. 134

of intelligence each having their own collection, analysis and counter-spy functions. In Great Britain however, various functions were assigned to different responsible agencies. The difference in approach saw the users in conflict with each other in Germany, and in Great Britain the suppliers fought.[59] These cases provide an example of the potential of an organisation to learn from historical experience.

However, there have been many cases where an organisation with ample access to the necessary information fails to learn from organisational history.

> The swine flu instance (1976) thus is crammed with negative examples, where the public health authorities and their superiors failed to turn organisational history to their account. But it was all around them, ready to hand.[60]

Levy defines experiential learning as "a change in beliefs (or the degree of confidence in one's beliefs) or the development of new beliefs, skills, or procedures as a result of the observation and interpretation of experience."[61] Intelligence is only as good as the value assigned to it by the users; history has once again provided a number of interesting cases. The prelude to the Nazi German assault on the Soviet Union in June 1941 demonstrated that the warning signals supplied by Soviet intelligence were ignored. The prevailing belief was that the Germans would not want to risk a war on two fronts.[62] A situation such as this implies the political role of the policy maker and high ranking official in the process, and that a 'failure' in intelligence may in fact originate at the political level and not from the IC.

So what are the reasons for seemingly 'neglecting' the historical experience of an organisation? There are a number of reasons that can be used to explain this situation. The first reason is related to bias, which is inherited in the process. There is a limited amount of time to ask the 'right' people. Those who are asked have a certain interest and knowledge about specific aspects and tend to highlight those. Secondly, it relates to the issue of speed. To get an objective picture of an organisation someone needs to look at the current resources, powers and personnel system, which is compared with the past. However, that same person needs to periodically ask the question "why". Thirdly, there not only needs to be knowledge about what an organisation does now, but also what it may and may not do in the future. Additionally there is also the human factor at play too, which requires patience in order to increase the chances of success. Pride may be another reason for failure. Incomplete, contradictory or imprecise results may also frustrate the process, which implies the need for a more systematic approach to institutional development.[63]

[59] Richard Neustadt and Ernest May, *Thinking in Time: The Uses of History for Decision-Makers*, New York, Free Press, 1986, p. 214

[60] Richard Neustadt and Ernest May, *op. cit.*, p. 219

[61] Jack Levy, "Learning and Foreign Policy: Sweeping a Conceptual Minefield," International Organization 48, 1994, pp. 279-312, p. 283

[62] Ernest May (ed.), Knowing One's Enemies: Intelligence Assessment before the Two World Wars, Princeton, Princeton University Press, 1984, pp. 536-7

[63] Richard Neustadt and Ernest May, *op. cit.*, p. 230

When it comes to the issue of organisational learning - not at the individual or simple organisational level a number of new factors need to be considered. How does policy making for the organisation, and the state it serves, differ from individual and organisational learning?

> The learning of a collective – a whole and complex entity such as a nation state – is different from the learning of an individual or a narrow decision-making group. Lessons must be internalised in some enduring, objective, consistent, and therefore predictable way. They may be institutionalised, embodied in new or revised procedures, preparations, dispositions; or they may take the form of new constraints or conditions that are added to the policy process. [...] Thus, learning a lesson means imposing upon the structure and process of policy choice a set of decision rules ("if-then" propositions), often in a concrete form, that will dispose the system to respond in certain ways – presumably better than before – to future contingencies.[64]

Therefore organisational learning as it is applied to the policy process of governments seems to be a compromise in terms of initiating change or innovation in order to meet a certain objective or problem. But the process is done within the context of understood 'rules' and boundaries, and the process should be ideally one with a predictable outcome. In the age of New Communication Technologies and the advent of 24/7 news, publicity also plays an important role in decision making, organisational learning and accountability issues. An event that is widely seen can exert a greater sense of urgency in politics (Vaughan 1996). This aspect adds an additional pressure upon policy makers, and one that they ignore at their peril.

Hedberg identified a number of different triggers for learning that are present in the environment in which an organisation operates. He states that an organisation cannot afford to continuously scan their environment, and only do this intermittently. The search is based upon an attention-directing standard operating procedure, which operates only as the result of problems beginning to build up. Affluence sometimes starts the search process, although it is more likely to be the result of; scarcity, conflict or substandard performance. Wealth, harmony and success tend to breed a culture of complacency and therefore reinforce existing behaviours. The triggers identified by Hedberg are:

- Problems,
- Opportunities,
- People[65]

One of the strategies that are promoted by Hedberg to facilitate organisational learning is through the promotion of experimentation. He states that: "if organisations are to survive in hostile and changing environments, they

[64] John Lovell, "'Lessons' of Military Involvements: Preliminary Conceptualization," in Donald Sylvan and Steve Chan (eds.), *Foreign Policy Decision Making: Perception, Cognition, and Artificial Intelligence*, New York, Praeger, 1984, pp. 129-157, p. 134

[65] Bo Hedberg, *op. cit.*, pp. 17-18

must change strategies and pursue new development patterns. Organisational designs should encourage experimenting so that organisations attain long-term viability."[66] Relating to the IC, the changing threat environment from the Cold War to post-Cold War threats is a good of the need for organisational learning and experimentation.

The Director of National Intelligence John Negroponte issued the *National Intelligence Strategy of the United States of America* in October 2005. A key assertion of the document was that the US IC must be a 'unified enterprise of innovative intelligence professionals.' It went on to outline how this transformation[67] was to proceed, based upon six mutually reinforcing and interdependent characteristics: 1) results focused; 2) collaborative; 3) bold; 4) future-oriented; 5) self-evaluating and; 6) innovative.[68] This document came in the wake of a lot of criticism aimed at the IC for their failures in 9/11 and the WMD case in Iraq from 2003. One of the criticisms faced by the US IC was that it failed to adapt to a changing environment. And therefore at the core of the problem is the issue of organisational learning.

Making Sense of the Theory

The theoretical discussion is structured in such a way as to take into account the various considerations that are not only required, but needed in order to bring about change and innovation in the IC. As such, the first stage is the realisation and identification of a problem or requirement – the framing of the issue is important in this respect. Without an urgent framing an issue is unlikely to get on to the policy agenda, the formulation.

It can be deduced from Stadler's *Four Principles of Enduring Success* that points three and four are the most relevant for the purposes of this paper. Point three on remembering your mistakes though is often externally driven and the results are imposed from an external agency, therefore relates more to the issue of change. Point four that concerns being conservative about change, which has implications for both innovation and change.

3. Empirical Views on Innovation – Four Cases

A major focus in this section will be on the challenges to intelligence organizations and adaptability to innovation during the post-Cold War-period. This period became – especially in US - a starter for fundamentally rethinking the intelligence process and requirements, when the threat picture shifted from a 180 degree view against the Soviet bloc to a 360 degree view against all kinds of

[66] Bo Hedberg, *op. cit.*,, p. 20

[67] In this regard, transformation is seen as the strategic process relating to bringing about an alteration in the IC, whereas innovation and change are seen as a subset of the transformation process.

[68] Glen Hastedt and Douglas Skelley, Intelligence in a Turbulent World: Insights from Organization Theory in Peter Gill, Steven Marin, and Mark Pythian, *Intelligence Theory*, New York, Routledge, 2009, pp. 112-130, p. 112

organisations (non-state actors) and states. Intelligence agencies started to execute economic espionage against traditional allied partners (for example France vs. US), and later on the new terrorism organizations challenged the traditional pattern on all aspects of intelligence - collection, analysis, dissemination and intelligence collaboration with earlier less desirable countries. Therefore the focus of the perceived threat gradually shifted from an ideologically charged grouping of states – the Eastern Bloc, to a period where there was a period of uncertainty who the enemy was after the collapse of the Eastern Bloc during 1989-91, and now consists of non-state terrorist organisations and a collection of 'rogue states' that have been coined the *Axis of Evil*.

Four cases of challenges - or more paradigm-shifts - will be looked at below which affected modern Intelligence Communities worldwide, and also called for organizational innovations – mostly from within. In the findings there will be some reflexions on similarities and differences on how US and Europe (UK) approached these challenges.

1. ***The Information Revolution and Open Source Intelligence***. Another fundamental change refers to the technological revolution where new IT-technologies and "mega-crawlers" created the first real serious competition to the Intelligence Communities of the world in being first and foremost with adequate information on political developments and crises.

   The United States Congress established the Aspin-Brown Commission (formerly known as the *Commission on the Roles and Capabilities of the US Intelligence Community*) in the wake of the failure of the 1992 National Security Act. OSINT came to the fore during a challenge posed by Robert Steele[69] to the IC, who could gain information on a nominated objective the fastest? The target was an African country. In the race, the IC used its secret sources and Steele used open source material. The end result was an embarrassment for the IC, which took considerably longer to get the necessary material: thereby putting into question the nature and means of information collection.

2. ***The Counter Terrorism-mission***. This is today the most important priority for almost all intelligence services. It also showed that no intelligence agency in the world has the required knowledge and understanding (anthropology, religions, language, cultures etc.) 'in-house'. The term 'academic outreach' became known as a way for intelligence services to tap into the voluminous research efforts within universities and think-tanks.[70] Private entities like Oxford Analytica in UK had already in the mid-90s found an economic rewarding way of funneling unclassified knowledge within academia to exclusive assessments for governments and leaders, but now the intelligence communities found that this is more than a niche complement to the existing working processes.

[69] See Robert D. Steele, *On Intelligence: Spies and Secrecy in an Open World*, Fairfax, VA, AFCEA, 2000

[70] See the Defence Intelligence Agency's mission statement with regard to education and research at http://www.dia.mil/college/mission.htm.

3. ***The increased need for pluralism and innovation in Intelligence Machineries***. Here the Israelis institutionalised a ”Devils Advocate”-model already after the Yom Kippur War as well as some change also came to daylight in UK as a result of false assumptions before the Falklands War. The need for pluralism became most obvious in both US and UK after the failed assessments on WMD as a precursor to the invasion in Iraq 2003. The ideas were around for a long time, but were given a new visibility when the CIA created a “Red Cell” for alternative assessments.

   An even wider endeavour to create second opinions and promote innovation and pluralism was the ID-8 proposal.[71] It was an attempt to overhaul the IC and turn the assessment and knowledge processes “upside down” with a primary focus to have an entry point in unclassified research within academia. It was thus intended to bring about radical changes to the system, but was halted due to bureaucratic obstacles and has ultimately not amounted to anything.

4. ***Approaching the new vulnerabilities in the Information Society***. When it comes to change in the Intelligence Community, it is not just a matter of considering what is being done in terms of domestic events and processes, which are considered. Of interest are what the Red Team is doing and may be planning to do. In addition to this, another angle needs to be factored in to the capabilities and intentions of Blue Team allies. This can be tied to the maxim of Sun Tzu in the *Art of War*, where he states that in order to be consistently successful on the battlefield one must not only know the enemy and their capabilities, but should also know one’s own capabilities. Given the level of interoperability within the context of the Global War on Terrorism, this insight is still highly relevant. Historically, for instance in 1932 Rear Admiral Harry E. Yarnell demonstrated the potential effectiveness of an air attack on the American fleet in Pearl Harbour. Nine years later the Japanese used almost the same tactics in destroying the fleet. A report from the exercise concluded that “*It is doubtful if air attacks can be launched against Oahu in the face of strong defensive aviation without subjecting the attacking carriers to the danger of material damage and consequent great losses in the attack air force.*”[72] Intelligence and insight is only as good as those with the foresight to use it effectively.

An explanation needs to be given at this point to justify why the UK equals Europe within the context of this article. Of course Europe is composed of much more than solely the UK. Reasons to include the United Kingdom are the long and experienced record (hence ‘old’) in the intelligence field, together with their ‘special’ relationship with the United States.

[71] Stollar, Larry., *ID8: New Approaches, New Solutions*, powerpoint presentation, April 2008

[72] Jack Young, The Real Architect of Pearl Harbour, http://findarticles.com/p/articles/mi_qa3834/is_200504/ai_n15743392/pg_3/, Spring 2005

3.1. The Information Revolution and Open Source Intelligence

Technology has become a part of everyday life, and this is no exception for the IC either. Information Technology (IT) forms one important aspect of technological information. IT was originally developed internally by the government for military use. However, the development of technological innovation by the open market has exceeded the internal development by the government and military.[73] A problem concerning the adoption of new technology has already been encountered.

Governmental adoption of technology has been faced with a problem, which is related to the responsiveness of governments in general. At times new technology is evolving more quickly than the governmental ability to adopt it. This demonstrates a need to decide and act quickly in order to keep up with the latest technological developments; it is a question of agility. There are those who warn against the reliance by the IC on IT. Lowenthal characterises the IT Revolution as being a means and not an end to the IC. He sees it as being more of an aid to perform tasks more efficiently, such as information-sharing, collection and collation.[74]

Quiggin notes that OSINT "if it is done correctly, it is as rigorous and timely as any other intelligence source and is usually done at a fraction of the cost."[75] Another advantage of OSINT is that it can be used to verify classified information without endangering the sources. For example the 1998 bombing of the al-Shifa pharmaceutical plant in Sudan.[76] This is merely one example, of the many, where OSINT could have proved its value. Publicly available information on the plant was overlooked in favour of a held belief that it was producing chemical and biological agents for al-Qaeda.[77] The case emphasizes the value of OSINT as a quick and cheap solution to a pressing problem.

Today's intelligent targets are smaller, more agile and mobile, and time sensitive. This must be reflected in the management and requirement systems.[78] The ratio of state secrets to open information was changing after the end of the Cold War. However, a deluge of OSINT changes the ways and means of collection. The emerging threats of the contemporary world are often asymmetric in nature. In this case, knowledge is power, and brute force alone cannot defeat the threat or release the populace from fear.[79]

[73] Mark Lowenthal, *op. cit.*, p. 307

[74] Mark Lowenthal, *op. cit.*, p. 308

[75] Thomas Quiggin, *op. cit.*, p. 157

[76] Amy Sands, "Integrating Open Sources", pp. 63-78 in Jennifer Sims & Burton Gerber (Editors), *Transforming U.S. Intelligence*, Georgetown University Press; 1st edition, 2005, pp. 70-71

[77] Jamie McIntyre & Andrea Koppel, *US Missiles Pound Targets in Afghanistan, Sudan*, http://edition.cnn.com/US/9808/20/us.strikes.02/, 21 August 1998 (accessed 28 August 2010)

[78] James Monnier Simon Jr., "Managing Domestic, Military, and Foreign Policy Requirements: Correcting Frankenstein's Blunder", pp. 149-61 in Jennifer Sims & Burton Gerber (Editors), *Transforming U.S. Intelligence*, Georgetown University Press; 1st edition, 2005, p. 150

[79] Thomas Quiggin, *op. cit.*, p. 231

An example of collection and collation innovation occurred in October 2009 it was announced that *In-Q-Tel*, the investment arm of the CIA had invested in *Visible Technologies* (http://www.visibletechnologies.com/), which is a "leading provider of social media analysis and engagement solutions."[80] *Visible Technologies* covers around 500 000 sites per day, listening to blogs and forums (Twitter, Flickr and YouTube for example), and trawling commercial sites with forums (e.g. Amazon) through a data-mining process. This venture seems to be an attempt by the CIA to be able to make use of open source information that is available on social networking sites (not Facebook though as this is a closed network).[81]

In a sector that is filled with sensitivities and secrets OSINT allows for greater flexibility. There are no secrecy issues, which is a distinct advantage when the IC has to deal with politicians, bureaucrats, foreign and domestic partners, and other agencies. There is a flip side to the OSINT coin. One of the problems identified is a growing reliance on the internet as a source of information, with no checking of the source, and information reliability or credibility. There is a tendency of analysts and policymakers becoming somewhat addicted.[82]

In 1996 the House Permanent Select Committee on Intelligence released a staff study – *IC21: The IC in the 21st Century*. It called for more 'cooperativeness' across the community and strengthened central management of the IC by giving the DCI additional administrative and resource authority. It proposed consolidating all technical collection activities into one large agency; refining the CIA's "centre" concept; creating two deputy DCIs (one for analysis and one for community management, including collection). However, there have been no radical changes, most changes relate to the management of the CIA. The IC continues to have a "stove-pipe" collection focus.[83]

The CIA had already began to explore the possibilities of setting up a centre within the framework of the organisation that used OSINT after the 1998 nuclear tests by India caught the IC off-guard.[84] John Negroponte created the Open Source Centre (OSC) when he was the DNI. Management responsibility went to the CIA. Some criticised it for being old wine in new bottles. The DNI

[80] Please see the Visible Technologies news release on the strategic partnership - http://www.visibletechnologies.com/press/pr_20091019.html.
To see the CIA blurb on Q-Tel go to - https://www.cia.gov/library/publications/additional-publications/in-q-tel/index.html. The In-Q-Tel website is found at http://www.iqt.org/.

[81] James Quilter, *CIA Invests in Social Media Monitoring Company*, Brand Republic, http://www.brandrepublic.com/News/947002/CIA-invests-social-media-monitoring-company/, 21 October 2009

[82] Thomas Quiggin, *op. cit.*, pp. 101-102

[83] Roger George and Robert Kline, *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Lanham, Roman and Littlefield Publishers, 2006, p. 58

[84] Scott Shane, *Intelligence Centre Is Created for Unclassified Information*, The New York Times, http://www.nytimes.com/2005/11/09/politics/09center.html, 9 November 2005

through the OSC tried to demonstrate the increased reliance on Open Source Intelligence (OSINT), such as the President's Daily Brief and NIEs.[85]

The US IC was formally established in 1947, after its necessity was understood following the onset of the Cold War. There have been a number of structural/organisational changes that have been instituted from above. In August 1960 the National Reconnaissance Officer was created by President Eisenhower. This meant that valuable intelligence assets would be jointly controlled by the Pentagon and the CIA. In 1996 the CIA was charged with the creation of NIMAC (National Imagery and Mapping Service, which has subsequently become the National Geospatial Agency (NGA)). The focus of these assets, as with the IC as a whole, is for supporting military operations.[86] An early realisation, judging from the events of 1960, demonstrates that stove-piping was a potential problem in this very young organisation, which necessitated organising the information collecting assets.

Information is the lifeblood of the IC. But what exactly is OSINT, and what is its role? Quiggin defines OSINT as being "an intelligence discipline that uses information of potential intelligence value that is generally available to the public." NATO use a very specific definition of intelligence and the role it plays, "information that has been deliberately discovered, disseminated, distilled, and disseminated to a select audience […] in order to address a specific question."[87] OSINT therefore brings flexibility to the intelligence system, which is needed given the changes in the nature of the current threat. Robert Steele's challenge to the US IC provided a clear example of the potential benefits to be derived from the 'new' form of collection, decisively outperforming the agencies in the time needed to gather sufficient information on a given case. According to the *NATO Open Source Intelligence Handbook*:

> OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a *select* audience, generally the commander and their immediate staff, in order to address a *specific* question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and *creates intelligence*.[88]

OSINT is not just a case of using the internet only. Deep web search techniques are used, which goes beyond the capacity of most web users. Some examples of programmes that are used includes: Lexis Nexis or Dialog.[89] The IT Revolution is a means and not an end for the IC. It is an aid to perform

[85] Mark Lowenthal, *op. cit.*, p. 303

[86] Thomas Quiggin, *op. cit.*, pp. 103-104

[87] Thomas Quiggin, *op. cit.*, p. 157

[88] *NATO Open Source Intelligence Handbook*, http://www.au.af.mil/au/awc/awcgate/nato/osint_hdbk.pdf, November 2001, pp. 2-3

[89] Thomas Quiggin, *op. cit.*, p. 161
To see a more comprehensive description of use of OSINT please refer to *NATO Open Source Intelligence Handbook*, http://www.au.af.mil/au/awc/awcgate/nato/osint_hdbk.pdf, November 2001, p. 1

tasks more efficiently – information sharing, collection and collation. (Lowenthal, 2009: 308) There are a number of emerging prejudices about OSINT, which imply that it can be performed by anyone and anywhere. This is more of a reflection of ignorance of the processes involved in the collection of information.[90]

One of the events that saw an effort to promote and drive the use of OSINT in the US was the Aspin-Brown Commission of 1996. They criticised the IC for failing to make greater use of OSINT. The Commission was established by Congress to review the IC's post-Cold War performance. Their findings indicated that the IC was moving too slowly in providing analysts access to open source data bases, particularly important owing to the deluge of information on the internet, for example.[91] The 9/11 Commission report of 2004 also mentioned the need to utilise OSINT more, to the extent of creating an open source centre in the CIA (but did not elaborate). In 2005 the WMD Commission released its report, and a similar recommendation to the 9/11 Commission, the establishment of an open source centre within the CIA. The WMD Commission also criticised the IC for under using OSINT. One of the conclusions of the 2005 report highlighted the problem.

> Analysts have large quantities of information from a wide variety of sources delivered to their desktops each day. Given the time constraints analysts face, it is understandable that their daily work focuses on using what's readily available — usually classified material. Clandestine sources, however, constitute only a tiny sliver of the information available on many topics of interest to the Intelligence Community. Other sources, such as traditional media, the Internet, and individuals in academia, non-governmental organizations, and business, offer vast intelligence possibilities. Regrettably, all too frequently these "non-secret" sources are undervalued and underused by the Intelligence Community.[92]

After the 9/11 Commission report in 2004, and before the WMD Commission report in 2005, Congress introduced an intelligence reform bill. One of the recommendations was for the establishment of an open source centre. The Intelligence Reform and Terrorism Protection Act of 2004 (P.L. 108-458) saw the most extensive changes to the IC since 1947, and an emphasis on open source information.[93] Thus there was a high level of political demand from the policy makers for establishing an open source centre, thus the change being imposed from the outside.

[90] For instance see http://www.oss.net/extra/news/?module_instance=1&id=2717 for Robert Steel's criticisms of the current state of OSINT.

[91] Richard Best & Alfred Cumming, *CRS Report for Congress: Open Source Intelligence (OSINT): Issues for Congress*, Washington DC, Congressional Research Service, 5 December 2007, p. 9

[92] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, March 31, 2005, p. 395

[93] Richard Best & Alfred Cumming, *op. cit.*, p. 11

It was decided to establish a National Open Source Enterprise, which was to embrace a number of key principles:

- the establishment of the position of Assistant Deputy Director of National Intelligence for Open Source with overall oversight responsibility of the open source effort;
- coordination by the Office of the Director of National Intelligence (ODNI) for open source funding requests in the DNI's budgetary submissions and allocations;
- the creation of a "Guild" of open source experts at an Open Source Centre and by ensuring that open source competency becomes an Intelligence Community requirement;
- a single open source requirements management system to balance resources and acquisitions against priorities;
- establishment of a single open source architecture to facilitate access to a wide range of potential consumers at federal, state, local, and tribal levels; and
- creation of an entity to develop and acquire cutting-edge technologies and processes that advances efforts to acquire and utilize open source information.[94]

On 1 November 2005 the National Open Source Centre (NOSC) was officially established. Officially it was established by the DNI, administratively speaking it is under the management of the CIA and its organisation incorporated and augmented by the Foreign Broadcast Information Service (FBIS). According to a DNI press release, NOSC's functions include the "collection, analysis and research, training, and information technology management to facilitate government-wide access and use."[95] This externally imposed change fits in with the type of change that is intended to erode rigid inter-organisational barriers in order to maximise the use of existing resources by pooling them together in a new structure.

NOSC provides information for all government agencies through access to the website www.opensource.gov. This information is in the form of translations and media transcripts from around the world, and other analytical products.[96] This helps to solve the problem of analysts having to look for the needle in the haystack, by placing all of the information in one place and not in dispersed locations.

This is a positive aspect, and touching on the issue of structural change and innovation, there are other aspects that need to be taken into consideration too. One of those aspects is organisational culture. This is not a question of making the physical task of access to information easier for analysts, but the

[94] Richard Best & Alfred Cumming, *op. cit.*, pp. 11-12

[95] Richard Best & Alfred Cumming, *op. cit.*, p. 12

[96] Ibid.

problem of the organisational attitude towards OSINT. Therefore some deeper searches need to be done. How does the IC, at the organisational level, value open source information? If it is undervalued or devalued, no manner of this type of change shall bring about the desired results of the policy makers.

Furthermore, Lowenthal identified one weakness of OSINT, which is that it is somewhat random with regard to its availability to all analysts.[97] OSINT is about information, and getting the right information to the right people in a timely fashion. This raises the issue of enabling a free flow of information in and between the IC organisations, policymaker and the end user. When it comes to information sharing among the various agencies within the US IC it is policies and culture, rather than technological barriers exist to the effective transfer.[98] There needs to be an increased emphasis on information sharing. This raises the question of which path to take in order to achieve this: develop policies that mandate information sharing and punish those who do not? In part this dilemma is answered by the organisational culture and organisational leadership, which is oriented towards secrecy in the case of the IC.

The UK efforts in the area of OSINT are less visible and more low-key. In the mid-1990s MoD created an Open Source office with Top Secret cleared librarians to better harness open source information and "grey" literature both within the domains of the MoD/Defence Intelligence Staff but also reachable from other parts of the UK Intelligence Community. The most important reason though for the absence of new forms of cooperation is probably the already existing informal partnerships with UK universities and the long tradition of academic outreach here. The tough information requests and needs second opinions on assessments could most often be solved through well – often personal "school tie" related – networks between intelligence officials and scholars.

In a comparative view between the UK and the US, the UK tends to make use of civilian experts and to fine tune existing means and mechanisms. This is in line with Stadler's first stated principle that is exploiting to the fullest extent innovations, to "exploit before you explore." The US approach to OSINT was an imitation and is relying on a technological approach that has been supplemented with the use of experts in the Global War On Terrorism (such as the use of anthropologists). The longer traditions of the UK are reflected in their approach to intelligence.

> The British also learned generations ago that obtaining pre-emptive information does matter when it comes to national survival, as they tried to navigate amidst the shifting alliances of European nations and their imperial ambitions. From time to time obtaining that advantage involved a degree of Machiavellian deception as well as skill and art, and even of cheating by way of seeing through the backs of the opponents' cards.[99]

[97] Mark Lowenthal, *op. cit.*, p. 303

[98] Mark Lowenthal, *op. cit.*, p. 308

[99] David Omand, *Securing the State*, London, Hurst & Company, 2010, p. 7

OSINT is about the processing of information and not the processing of secrets. This has come about, as previously stated, as a result of the culmination of a number of circumstances and changes in the intelligence and threat environment. Therefore this raises a vital question; is OSINT an innovation or a necessity? In order to answer this question it is vital to revisit the input versus output argument, where NPM focuses (as does Stadler) upon the result rather than the process. The current threat environment that the IC needs to accurately analyse and understand quickly, OSINT in this regard can be considered as being an innovation within the input part of the process. Given the nature of current threats, especially asymmetrical threats that evolve and emerge rapidly, OSINT can also be considered a necessity in this regard.

3.2. Counter-Terrorism

The issue of counter-terrorism had already begun to emerge as a priority for the IC by 1994-95 with the emergence of groups, such as al-Qaeda. In 1993 the attack on the World Trade Centre in New York was a hint of the 'new' type of global threat to come. This has been reinforced over the years with a string of attacks across the globe, and eventually bringing the threat to the rest of the world from 9/11, to March 2004 in Madrid and London in July 2005.

The opponent facing the IC is very adaptable and unpredictable. The dilemma facing intelligence agencies is that they need to be successful 100% of the time, which places a great deal of stress and burden. For if an attack is successful or some other kind of failure occurs, the legacy of years of success is soon forgotten. In terms of an event having a transforming effect upon the United States IC, the impact of the Iraqi WMD yielded a greater impact on the transformation of analysis than 9/11.[100] This tends to support the saying that the greatest learning comes not from successes, but from defeats and setbacks.

One of the innovations from within the IC is the creation of the red cell/blue cell concept. Originally the red cell was used during the period of the Cold War as a means to try and understand how the Eastern Bloc countries thought, thereby being able to anticipate the enemy. After the Cold War the red cell/blue cell concept has been adapted to a role in counter-terrorism.

9/11 proved to be an event that caused a significant amount of reflection upon the task of analysis. The United States as a leading player in the Global War On Terrorism not only needs to consider and understand what the enemy is thinking and doing, but also the thinking and capabilities of their own assets (and those of their allies). This needs to be done through expanding the world view of the organisation. A Cyber Defence Exercise in 2006 illustrates the potential roles played by the cells, in this case in training.

- Blue Cell participants included students of computer science and related fields at the nation's military service academies. Their role was to defend the

[100] Mark Lowenthal, "Intelligence Analysis: Management and Transformation Issues", pp. 220-38 in Jennifer Sims & Burton Gerber (Editors), *Transforming U.S. Intelligence*, Georgetown University Press; 1st edition, 2005, p. 232

military network.

- Red Cell participants played the aggressors. They came from the NSA and various service network security groups such as the Air Force Information Warfare Centre at Lackland Air Force Base in San Antonio, Texas, the Navy Information Operations Command at Fort Meade and the Marine Corps Network Operations and Security Command at the Marine Corps Base in Quantico, Virginia.
- White Cell participants, also seasoned network security professionals, acted as exercise proctors, referees and scorekeepers.[101]

Moving beyond the classroom and to a practical application of the red cell, further complexities get introduced to the equation. The testimony of Bogdan Dzakovich to the National Commission on Terrorist Attacks Upon the United States in 2003 was very revealing of the role of the work of the red cell in not only understanding how the enemy thinks, but also in testing how blue forces react to breaches of security. The red team was established in the wake of the bombing of Pan Am 103 (before the end of the Cold War!) by the Presidential Commission who directed the FAA to develop "measures to improve testing of security systems." TWA 800's crash off New York and the 1996 FAA Reauthorisation Act (P.L. 104-264) further reinforced and defined the red team role. In particular, emphasizing that "… the Administrator (of FAA) shall conduct periodic and unannounced inspections of security systems of airports and air carriers to determine the effectiveness and vulnerabilities of such systems …"[102] These statements show that an awareness existed of the vulnerabilities, and an attempt was being made to plug them with the use of red cell strategy.

Dzakovich was extremely critical of the FAA though, which was increased after the 9/11 attacks. He went as far as to state in the Commission hearings that the FAA embarked upon a plan of deception to cover up their incompetence and culpability in this failure.

> What happened on 9/11 was not a failure in the system, it was a system designed for failure. FAA very conscientiously and deliberately orchestrated a dangerous façade of security, ignoring the laws cited above. They knew how vulnerable aviation security was. They knew the terrorist threat was rising, but gambled nothing would happen if we kept the vulnerability secret and did not disrupt the airline industry.[103]

In spite of a number of warnings, in terms of events and whistleblower testimony, there was no change within the FAA or any attempts to right the defi-

[101] Todd Lopez, *Military Students Get Lesson in Cyber-warfare*, Security News, Search-Security.Com, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1186049,00.html, 3 May 2006 (accessed 26 April 2010)

[102] Statement of Bogdan Dzakovic, National Commission on Terrorist Attacks Upon the United States,
http://www.9-11commission.gov/hearings/hearing2/witness_dzakovic.htm, 22 May 2003 (accessed 26 April 2010)

[103] Ibid.

ciencies. Outside agencies that are intended for oversight, such as the Department of Transportation's Office of the Inspector General either ignored or did not follow up on findings. There was a demonstrated tendency towards institutionalised secrecy; it was organisation culture and psychology, rather than the innovation that ultimately resulted in the failure. The use of red cell/blue cell, if it is implemented and run properly, provides a safe environment in which to test and formulate strategies and responses to possible threats.

What are the experiences of other countries, when it comes to change and innovation in the IC, with regards to meeting terrorism? British counter-terrorism (known as CONTEST – Counter-Terrorism Strategy) is based upon the principals of the Four Ps, according to the Office for Security and Counter-Terrorism (British Home Office) the strategy has four key elements:

- Pursue - to stop terrorist attacks
- Prevent – to stop people from becoming terrorists or supporting violent extremism
- Protect – to strengthen our protection against terror attack
- Prepare – where an attack cannot be stopped, to mitigate its impact

These four areas of work complement and reinforce each another to reduce the terrorist threat to the UK and our overseas interests.[104] British strategy in combating terrorism relies on a mix of reactive and proactive measures. The long experience of fighting terrorism, based on the lessons learned from the Northern Ireland experience seem to give an edge over their less experienced US counter-parts.

The bombings in the UK on 7 July 2005 caused the policy makers to undertake a series of reviews of the performance of the UK IC, including the Comprehensive Spending Review of 2007 (CSR07 – led to an increase in funding available to the Agencies to just under £2 billion by 2010/2011).[105] According to the Intelligence and Security Annual Report the focus is on the pursue aspect of CONTEST.

Structural re-organisation has been undertaken by the UK in order to maximise the performance of the IC, through avoiding such issues as stovepiping and organisational compartmentalisation. An example of this was the creation of the Internet Operations Centre (INOC) in 2008. INOC brings together all of the Government Communications Headquarters (GCHQ) computer network operations capability into a single team in support of internet-related counter-terrorism operations. According to feedback, the result has been a success.[106]

[104] *Counter-Terrorism Strategy*, Office for Security and Counter-Terrorism, http://security.homeoffice.gov.uk/counter-terrorism-strategy/about-the-strategy1/four-ps/index.html, 14 March, 2010

[105] Kim Howells (Chairman), *Intelligence and Security Committee Annual Report 2008-2009*, Norwich, The Stationery Office, 2010, p. 4

[106] Kim Howells (Chairman), *op. cit.*, p. 8

There are a number of similarities here with the changes and innovations undertaken within the US IC.

One of the initiatives that seem to have gained currency is the creation of joint task forces and centres in order to try and erase the institutional barriers that would otherwise exist. This is being done in both the United States and the United Kingdom. Some of the results of this new thinking and organisational structure include: Joint Terrorism Task Force (JTTF), Terrorist Threat Integration Centre (TTIC - succeeded by NCTC in 2005), Joint Terrorism Analysis Centre (JTAC) and the US Interagency Intelligence Committee on Terrorism (IICT). Interesting here is that JTAC was first in it´s kind of a real operational fusion centre and several years ahead of the US version NCTC became the model. The UK model has since also been followed by most other European countries like France, Netherlands, Denmark etc.

A recent article appearing in the Washington Post (see footnote 1) gave a hint of a new innovative focus in tactics used by the CIA in counter-terrorism, but at the same time highlighted some of the 'old' thinking that constrains the US IC. According to the CIA Director Leon Panetta there would be "more co-location of analysts and operators at home and abroad" over the next five years, and that the fusion of the two "has been key to victories in counterterrorism and counter-proliferation." Yet simultaneously there was talk of protecting the CIA's turf.[107] This demonstrates a certain erosion of the intra-organisational walls, in having operators and analysts working together, but shows that the inter-organisational walls still very much exist.

3.3. Policy imposed innovations - ID 8 and PIU

In the wake of 9/11 and the Iraqi WMD debacle Congress and Blue Ribbon panels called for a broad based reform of the IC. The DNI pushed forward its own set of initiatives for a far reaching reform programme. A discussion arose about the necessity of creating 'catalyst' initiatives in order to be able to meet the IC's daily challenges and demands. DNI Director Hayden addressed his workers on the planned changes.

> We are going to establish a new venture where our officers will work with people from academia, the private sector [...] to create new ways of doing business. Its mission will be to help us, CIA, tackle our hardest, most-enduring, and over the horizon challenges [...]
>
> We want to encourage real innovation and creativity, so, in essence, we're going to take this structure, and we're going to liberate it from the mother ship [...]We are going to let people we've assigned to do this explore new approaches, new tools, and new relationships.
>
> It will be experimental. It will be directorate-less. It will be fully integrated.

[107] Greg Miller, *CIA to station more analysts overseas as part of its strategy*, Washington Post, www.washingtonpost.com/wp-dyn/content/article/2010/04/29/AR2010042904355_pf.html, 30 April 2010

> It will be self-organising. It will be autonomous.
>
> It will design its own IT infrastructure. It will design its own HR management framework and other business processes that it needs. They will not be required to mimic or to be constrained by long-standing practices here at the main campus […]
>
> The idea is to give this venture the freedom to see what works, and to challenge some of the premises we have back here […] I expect it to make a few waves, but its kind of designed to do that.[108]

A proposal was made by the WMD Commission report in 2005[109] to free up the access to and flow of information, for which it criticised the US IC. The philosophy behind ID8 (derived from the word ideate – to create ideas) is that it operates in a 'borderless' open and sharing environment, where 'real' solutions are sought for 'real' problems. It came about as a result of a perceived IC failure, and the resulting political pressure to try and minimise the chances of that failure occurring again. Therefore this is an attempted form of change that has been initiated from beyond the organisational structure of the IC in the United States. The idea is that the organisational structure should be small in order for it to remain agile and innovative.

A reality since the 1990s is the growing capacity of the private sector, which can have more knowledge and expertise on a given issue of national security than intelligence agencies. It is an age of "distributed intelligence" rather than "centralised intelligence."[110] In an era of diminishing government finances and resources there is an increased need to cooperate with services and knowledge that are relatively expensive skill sets, which necessitates collaborating with private enterprise and academia. As noted by Director Hayden, it is a novel and potentially controversial move for the IC (initially due to pre-existing mindsets and arguments).

The CIA's ID8 programme was described by RAND Corporation's Gregory Treverton as being born from a need to create an agile and adaptable organisation in order to effectively meet the new threats and challenges.

> One CIA proposal, unhappily struck with the moniker ID8, would approach hard intelligence problems much as my own institution outside the government, the RAND Corporation, does: It would first reach to the outsiders in academia, think-tanks, and Wall Street. It would work at the unclassified level, only classifying work if it absolutely had to.[111]

Treverton proposes further that organising by problem or mission as opposed to information source or analytic agency would bear results (espe-

[108] Director Hayden address to the workforce, 2 October 2007

[109] To access the unclassified version of this report, please see: http://www.gpoaccess.gov/wmd/index.html.

[110] Thomas Quiggin, *op. cit.*, p. 165

[111] Gregory Treverton, *Intelligence Test*, Democracy: A Journal Of Ideas, www.democracyjournal.org, Winter 2009, p. 62

cially in breaking down barriers between collector and analyst).[112] The current distinctions and separations that are built in to the current IC structure are actually an impediment, rather than an asset. He implies a potentially fruitful relationship between the IC and other institutions or spheres not usually associating with each other.

Academic outreach is an innovation based upon the various constraints imposed upon the state in the contemporary political and economic context. In mid-2008 a DNI directive defined the term 'outreach' as being "the open, overt, and deliberate act of an IC analyst engaging with an individual outside the IC to explore ideas and alternative perspectives, gain new insights, generate new knowledge, or obtain new information."[113] This is a means to have access to specialised services and knowledge without the expense of maintaining them as an integral part of the organisation, especially when placed within the context of the ideals of the New Public Management philosophy adopted by some governments.

The use of Outreach in the US IC is not a new concept or practice. An example of Outreach in the US can be found in the late 1940s, the CIA's Board of National Estimates formed the *Princeton Consultants*. This was a group of distinguished professors who met with the Board in secret at Princeton several times in a year in order to draft intelligence estimates.[114] Such collaboration between the IC and an external partner was rare due to the secretive nature of the IC, and demands a great deal of trust in order to be effective.

The final result has not been overly promising though, in spite of a lot of promise to begin with, organisational culture within the IC has proved to be the biggest obstacle. In the words of Patrick Neary, "ID8 hangs on by a thread."[115] This fact demonstrates that there is much more work to be done on breaking down the rigid boundaries between the different agencies that makes up the IC.

In addition to understanding the theoretical approaches to innovation and policy by the academic community, given the nature of this work, it is critical to understand this problem from the point of view of bureaucrats and administrators within the government machinery. A hint at how bureaucrats and administrations in the UK addresses the problem of formulating and implementing policy can be found in novel approaches to finding the 'best' ways of going about this task. In July 2000, the Policy Innovation Unit was established by the Northern Irish administration. The role for the Policy Innovation Unit (PIU) was described as being:

- improving the administration's capacity to address strategic, cross-cutting

[112] Ibid.

[113] U.S. Intelligence Community Directive 205, "Analytic Outreach", http://www.dni.gov/electronic_reading_room/ICD%20205.pdf, 16 July 2008

[114] Gregory Treverton, *Approaches to "Outreach" for Intelligence*, Stockholm, Swedish National Defence College, 2009, p. 6

[115] Patrick Neary, *Intelligence Reform, 2001-2009: Requiescat in Pace?*, Studies in Intelligence, Vol. 54, No. 1, March 2010, pp. 1-16, p. 14

issues;

- promotion of good practice and innovation in the development of policy and in the delivery of the administration's objectives, informed by best practice elsewhere; and
- the promotion of evidence-based policy making, including the dissemination of relevant information and research.[116]

Although this is at the regional level of government, the stated objectives give an insight into the larger world of policy making from a bureaucrat's and practitioner's point of view and approach to policy formulation or imitation. From the wording used to describe their function, the PIU seem to approach the idea of innovation as being some way of doing something, which currently does not exist here. So therefore innovation is not necessarily an idea, technique or technology that currently does not exist at all, but may be existing and just 'imported' as a means to solve a policy problem. This may be symptomatic of the idea 'if it works over there then it should work here' approach, which may not necessarily take into account local conditions that may necessitate some adaptation of the policy for it to be effective.

3.4. Approaching the new vulnerabilities in the Information Society

Foryst posits seven major characteristics of the US IC that seems to guide the result of the final intelligence product and could be constraining creative and imaginative thinking. She lists these as being: defensive thinking; stale assumptions; reactive posture; constrained imagination; no national strategy; constrained perceptions and; failures.[117] What she argues for is a "Total US" approach to intelligence. The idea is to have the IC working in conjunction with each other (between agencies and departments) in order to improve the quality and relevance of the final intelligence product, to both the government and the wider community.[118] A relevant point made by Foryst is the need to be aware of one's own weaknesses and short comings and not only the object of intelligence gathering and their intentions and capabilities – sometimes also done within the frame of "net assessment". This is an evolutionary process (as opposed to revolutionary process) with the new Homeland Security requirements for the IC.

This is in reality also a kind of critique to the first phase of US organizational responses to 9/11 with the creation of the Department of Homeland Security built on big chokes of other existing agencies with no coherent cultures. DHS

[116] Policy Innovation Unit, Office of the First Minister and Deputy First Minister, Northern Ireland Government, http://www.ofmdfmni.gov.uk/index/economic-policy/policy-innovation-unit.htm, 21 July 2009

[117] Carole Foryst, *Missing from US Intelligence Analysis: The Concept of "Total US"*, in International Journal of Intelligence and Counter-Intelligence, Philadelphia, Routledge, Volume 22, Number 3, Fall 2009, pp. 396-420, pp. 398-400

[118] Carole Foryst, op. cit., see especially pp. 415-418

would probably be ideal to be in charge of "blue" vulnerabilities assessments which then should be interfaced with the IC:s "red assessments".

The United Kingdom has managed to draw upon a wealth of experience in dealing with crowd and transport related disasters from the 1980s and 1990s, in thinking about the task of CIIP (Critical Information Infrastructure Protection). These lessons taught that no one single agency has the ability and resources to respond effectively to a disaster involving CNI.[119] 11 September 2001 in the United States and 7 July 2005 in London, highlight the fact that 'conventional' terrorism still poses a significant risk for society and the government. But there have been other events, which demonstrate the emergence of a new threat (which was predicted some time ago as a possibility), with attacks on Critical Information Infrastructure (CII) in the UK. To illustrate the level of the problem there was a news report stated that in 2005, "nearly 300 UK government departments and businesses critical to the country's infrastructure were the subject of Trojan horse attacks, many reportedly originating in the Far East."[120]

An innovation to address this electronic threat was announced when MI5 hired some 50 hackers that forms part of the newly established and top secret Cyber Operations Command. Jonathan Evans, the head of MI5, has made a number of public statements regarding the cyber threats faced by the UK. He has alleged cyber terrorist threats emanating from China, Pakistan and Russia.

Evans also alleges that messages to terrorists in Belmarsh Prison have been intercepted; stated in a report to the Security Minister Lord West that some 1000 attacks were launched on Whitehall computers in the summer of 2009 (other targets were air traffic control, power stations and the City of London); he sent a confidential memo to some 300 banks and accounting firms warning that they were already under attack by Chinese state organisations. Lord West has characterised these new government hackers as being "youngsters who use their talents to stop other hackers from closing down this country."[121] In this particular organisational innovation, human technological knowledge is used as a means to help defend the UK's vulnerable Critical Information Infrastructure from attack. It also fits with the English saying that the best gamekeeper is a former poacher.

The issue of CIIP and Defensive Information Warfare raised a heightened interest in 1994-95, but was debated in its early forms in the UK already by 1990. The developments are unfortunately not that publicly traceable as UK sorted these issues much to the domains of its intelligence community. NISCC

[119] *Critical Infrastructure Protection and Crisis Management in Britain*, IAAC Briefing Paper, No. 14, 8 January 2001

[120] *Fingers Pointed at Chinese Military After Hacking Reports*, Sophos, http://www.sophos.com/pressoffice/news/articles/2007/09/chinese-hack.html, 5 September 2007

[121] Gordon Thomas, *Mi5 Hires Teenagers to Battle Cyber Terrorism*, Daily Express, 20 September 2009 in James Harley, *Information Operations Newsletter*, Volume 10, No. 02, 2009, pp. 4-5

was in reality a virtual coalition with a small staff of its own and technically dependent on the Central Electronic Security Group (CESG) – the information assurance branch of the UK signals intelligence agency GCHQ in Cheltenham. As NISCC was housed within in the British Security Service (MI5) it seemed natural that this organisational part later merged with those within MI5 that was responsible for physical protection, to a branch called Centre for Protection of National Infrastructure (CPNI) some years later. Now it seems that the Cyber-Protection parts of MI5 once again been reorganized to the new Operations Centre in Cheltenham. All of this points to a certain degree of organizational innovation or at least adaptability within the UK IC.

These changes in the UK reflect a new way of looking and assessing the effectiveness of governmental structures. A recent article in the British media outlet *The Guardian Public* showed the new criteria used by the Cabinet Office in its capability reviews of government departments (including the GCHQ). Those criteria are:

- Innovation;
- Collaboration;
- Value and delivery;
- Results.[122]

This restructuring and assessment of the UK capability when it comes to the Homeland Security/CIIP-affairs seems to fit with the notion of core government businesses taking on a more 'business-like' approach to their tasks, which fits with elements of the NPM approach. It also fits with Stadler's first principle, which is to try and get the best from the existing innovations before inventing new ones. These changes in the British and American system fit with what the US Director of National Intelligence John Negroponte characterised as being "institutional innovation" in 2006. He stated that it shall take time "remaking a loose confederation into a unified enterprise." And that "institutional innovations, most of which are system-wide procedural improvements" are intended to "optimise the community's total performance."[123] It can also be seen as an attempt to try and redress the problem of the IC being a 'Frankenstein's monster' – each part working fine individually, however dysfunctional as a whole.

3.5. Findings

These case studies represent an explanatory study where the main focus of the research is on the United States IC, examples from the UK serve to place the changes in the US IC into context. The specific context being the US is an example of a newly established IC and the UK as an example of an established

[122] Jane Dudman, *Cabinet Office Updates its Capability Reviews*, www.guardianpublic.co.uk/capability-reviews/, 16 July 2009

[123] Walter Pincus, *Negroponte Cites 'Innovations' in Integrating Intelligence*, The Washington Post, A07, www.washingtonpost.com, 21 April 2006

IC. Does this affect, in addition to other factors, the approach to change and innovation? One thing that is in common with policy in both the UK and US ICs is that there is a tendency to be conservative about change, which is in agreement with Stadler's fourth principle.

The introduction hypothesized that the United States should have the lead in innovation, which should be based upon their technological and resource base, over their European counterparts. An example of this is certainly demonstrated by such innovations as In-Q-Tel. However, this is balanced by the experience, for example the British in Northern Ireland, which gives them an edge in organisational innovation. The Policy Innovation Unit gives an example of this kind of innovation, from an organisational sense. This seems to be an adaptation based on the more constrained financial resources available in the UK, where new technology is expensive and other means are attempted to try and get the best out of the existing system.

The general finding from these four cases is thus that while the Americans try to build new organizational layers on existing organisations to coordinate them, the British tend to build on the existing ones and force them to cooperate smother or in a new fashion. The British JTAC was the first real CT-fusion centre and was based on secondments from existing agencies, while the US NCTC was more seen as "a new kid on the block" – similar to DHS mentioned earlier – and early became involved in turf fights with other organisational elements who had overlapping missions still residing in the existing intelligence and law enforcement organisations. The greater amount of financial and technological resources available in the US allows the luxury to explore new innovations, rather than the British approach of exploiting existing innovations. The US when measuring performance, to an extent is still focused upon the issue of focusing upon inputs, whereas the UK is much more oriented to outcomes. This may be a reflection of the fact that NPM has been a key component of public management in the UK for some decades, but has not taken in the US.

This organizational adaptability can also be seen as a counterargument to the earlier assumption that the "young" US IC has a lead vs. the "old" European ICs when it comes to innovation, i.e. that US innovates and Europe imitates. By a 'young' US IC this refers to its creation in 1947 as opposed to European ones. For example the British IC has been established in a formal sense since 1909, but has existed since the times of Queen Elisabeth 1st. There is a link between the IC, the Presidential administration and academia in the United States. The US system is also guided by key personalities and clearances, and there is also movement of people between agencies whereas there are more established routines and traditions in Europe, and less movement between agencies. Additionally, universities in the UK are more independent than in the US owing to their more favourable financial situation.

Reflecting upon the theoretical perspectives of this paper, which of them are present in these case studies? There are certainly some elements of the New

Public Management philosophy in the process of change and innovation in the IC. Although this is not uniform and it is in a number of cases not complete (in realising the goals of the policy toward the intended change or innovation). One of the greater impediments is the secretive nature of the IC, which means making the institutions more publicly accountable through reducing bureaucratic control is very problematic. Making the IC a money making enterprise has its problems too, especially considering the likely primary customer is the government. NPM is useful to a limited extent owing in no small part to the fact that the IC is not an open and competitive commercially-oriented environment. There is still a relative lack of civilian control and public transparency owing to the various associated sensitivities.

Having said this, the process of change and innovation through policy, as defined by Harrop is a three stage process – initiation, formulation and finally implementation. A number of reforms have stumbled through this process, but others get 'stuck' along the way, such as the ID8 proposal. Metcalfe's points on the challenges facing governments in public policy management have been surfacing – the fast pace and type of change faced; and governments operate through networks of interdependent organisations (as opposed to independent ones in the business world). The IC has faced a very rapidly changing threat environment and the changes required to effectively meet these 'new' threats are massive.

Some techniques and methods have been borrowed from the business world, such as Stadler's *Four Principles of Enduring Success*, whether this is intentional or a logical step is another question. The third and fourth principles are the most easily observed within the context of change and innovation within the IC. There is often a conservative approach when it comes to the nature and magnitude of change and innovation, which is often undertaken in small steps. The failures of intelligence in 9/11 and especially with regard to Iraq (weapons of mass destruction assertion), have brought about governmental commissions and inquiries to explore the root causes.

All of these above are contingent upon organisational learning though. These changes and innovations are born from the ability of organisations learning from their successes and failures and to initiate formulate and implement the appropriate policy for the required and intended practical outcome. However, the effectiveness policy is tempered by the political process as noted by Lovell, where negotiation and bargaining often waters down the original proposal.

Hedberg identified three triggers to learning – problems, opportunities and people. The cases here illustrate that these three triggers are valid in influencing change and innovation in the IC. The changing threat environment in the post-Cold War period has been a catalyst for making changes and innovations in the IC. The asymmetric threats that have emerged require a much quicker and accurate response. This has also given rise to opportunities, in this regards

OSINT is an opportunity. Making use of non-classified information has a number of advantages in collection and dissemination. It is much quicker and the lack of secrecy enables a more efficient spread. People have also proven to be decisive, someone that is prepared to take the risk in instituting innovation and change. President Eisenhower in the US in creating the US IC provides one example.

4. Conclusion and Summary of Findings

Governments are looking more and more to the business community for inspiration and ideas on how to reform and reshape their way of doing business. NPM is one such idea that has gained currency in the Anglo-American world of public management. It emphasizes a leaner and more efficient way of doing business, where the final product is more important than the inputs. Moving on from the broader theory, Stadler moves into the specifics of organisational success. One of his four principles stresses the importance of utilising existing innovations to their fullest potential.

An observation and conclusion by a group of European researchers on institutional design in public institutions was that policy is being directed at survival, but a design that is intended for adaptation. "The best that designers may be able to do is to endow an organisation with sufficient flexibility to adapt."[124] This provides a good explanation as to why changes are often made in small and incremental steps.

The UK IC shows a greater tendency towards utilising the philosophy and practice of NPM, when it comes to bringing about change and innovation. They also try to fine tune and improve existing assets and capabilities, which was proposed by Stadler. This seems likely to be a reflection upon the budgetary constraints faced by the government. Certainly this contrasts significantly with the US IC, which faced significant criticism in the Washington Post article for being bloated and inefficient. The US approach to change and innovation in this light seems to be instigated through the aid of significant cash injections, but the effort is poorly guided and coordinated. A tentative conclusion, which requires further investigation, is that governments that are more able and/or willing to invest in large budgets tend not to follow NPM than governments that are faced with budgetary constraints.

The lessons drawn from organisational learning demonstrate that the policy process of bringing about innovation and change is not necessarily a rational one, which applies the best remedy to the identified problem or error. It is a process that is watered down by bargaining and politics, especially in a sensitive field as intelligence. A number of other factors in the organisation and

[124] Arjen Boin, Sanneke Kuipers & Marco Steenbergen, *The Life and Death of Public Organisations: A Question of Institutional Design?*, Governance: An International Journal of Policy, Administration, and Institutions, Vol. 23, No. 3, July 2010, pp. 385-410, p. 404

the state which it serves also play a part, especially the issue of personnel that constitute the IC, together with their interests and biases.

First and foremost in the contemporary world, the IC serves to realise the foreign policy interests of the state. Gregory Treverton puts this succinctly when he states that the IC is designed to serve American foreign policy. It also needs to adapt to a rapidly changing world.[125] This means that the IC needs to transform in order to meet this changing environment in order to meet its objective of supporting foreign policy.

The debate on the reform of the intelligence sector has proven to be somewhat inconclusive to date. This is reflected by Lowenthal's conclusion about intelligence reform. "The intelligence reform debate has an inconclusive aspect, which reflects both the difficulty of the issues and choices involved and the boundless enthusiasm of reform advocates, particularly those outside the intelligence community".[126] One of the major dilemmas is that certainly improvements in terms of better efficiency and new objectives or goals can be strove for, but just how this is achieved in practical terms is more elusive. Changes may also have the potential to do more harm than good too.

Therefore innovation offers a relatively good and lower risk means of improving the structure and the processes of the IC. These are often initiated internally and are intended to meeting a changed threat environment, for example. In terms of innovation, it can be used to affect organisational structures or processes. The opportunities and abilities to innovate are tempered by politics, priorities and resources.

One focus of this article has also been looking for similarities and differences between the United States and Europe. At a glance, one may expect that the United Kingdom may fall somewhere in between Europe and the United States due to their 'special relationship' with the United States. This involves understanding political priorities and perception of threat by not only the defence and intelligence sectors, but by the political decision-makers as well. The US has a tendency to use its advantage in terms of technological and resource superiority as a means and basis for innovation in the IC. The European IC, which has been established a lot longer than their younger US counterparts, face an obstacle of having fewer resources and technological innovations at their disposal. Instead there is a focus on organisational innovation that has been derived from experience, such as the British experience in Northern Ireland.

Overall though, it seems that the US IC have clear prerequisites for a greater adaptability and pluralism at large, but where change and innovation unfortunately often seems to end up in a new organizational layer or entity without reducing any of the old ones causing coordination and efficiency issues. Some

[125] Gregory Treverton, *Reshaping National Intelligence for an Age of Information* (RAND Studies in Policy Analysis), Cambridge University Press, 2008, p. 20

[126] Mark Lowenthal, *op. cit.*, p. 311

of those to US favourable factors/prerequisites here that could be mentioned are:

- Lower entry/exit-barriers on the labour market in general ("Hire and Fire").
- The tradition of "Academic Outreach" which is coupled with a fluidity of scholars moving between universities and think-tanks, the Intelligence Community and positions within the executive branch.
- Another reason for these lower barriers between the institutions above which also could be seen as reinforcing pluralism, is the system of personal clearances in US compared to the dominating system of clearances due to (a government) "position" within Europe. This means that you could have real access while working for an independent think-tank on a government sponsored study.
- Wealthy universities and tax-reduction on private economic sponsoring to non-profit organisations like think-tanks. Former key officials thus have an economic incentive to – maybe just for a while - take up a position outside government and still have an impact on government and intelligence assessments. This doesn't exist in Europe in general where the existence of independent think-tanks in this area is a rare phenomenon and the universities generally are "poor". UK could here be seen as a possible exemption with wealthy universities and thus also with some tradition of "low-key" academic outreach as a lot of specialist are residing there. In other European countries a scholar could double his/her salary by joining their national Intelligence Service, which not exactly is promoting pluralism in the sense above.

A final word on bringing together the concepts of innovation and organisational learning in terms of the lessons learned and applied through policy is the question that further needs to be asked. The question is not about whether the innovations or change have improved and reduced the chances of an 'error' occurring again in the future. There are a lot of compromises that occur along the way of the policy process, including political priorities and political compromise, and the availability of sufficient resources to realise what is planned.

Article 3

Information Terrorism - When and By Whom?

Published in
Defense Intelligence Journal
(Vol. 16, No. 2, 2007, 139-154)
by National Defense Intelligence College Foundation, Inc.

Abstract

This paper examines the phenomena of information- and cyber terrorism - within the greater framework of "functional terrorism" (means/methods) – with definitions, cases, trends etc. The thesis established here is that the trends of traditional (kinetic) terrorism and information terrorism will likely merge, despite the fact that an information terrorism act has yet to be executed. The question in focus is thus not "if" but "when," which this paper tries to elaborate on. The paper concludes with some remarks on indications and warnings as well as on actions and policies that might be taken to counter information- and cyber terrorist planning and attacks.

Keywords: Homeland Security, (Defensive) Information Operations, Terrorism, Infrastructure Warfare, Information Warfare Techniques, Counter-Intelligence

Introduction: Information Terrorism – When And By Whom?

The convergence between terrorism and information operations is a hotly debated issue. Even if we haven't seen such actions executed yet, the imminent issue is not "if" but "when." When will terrorists move beyond mere physical acts of mayhem and destruction towards exploiting our societal vulnerabilities in our modern information society in efforts to cause chaos, panic and economic paralysis? If this occurs, what is the likely time-scale when an attack will take place? Will it occur within one year, five years or within the next decade?

Judging exactly when a terrorist group may suddenly transform and take the leap between using cyberspace as a force-multiplier mechanism for enhanced command, control, communication and information-gathering purposes into an offensive cyber weapon is still relatively unchartered territory. There is certainly a trend of "known" incidents that seem to suggest that terrorists are moving in this direction. What is clear is that cyberspace has fundamentally shifted the security landscape, both in terms of our capabilities and vulnerabilities as increasingly networked societies. This complicates our ability to map calibrated threats onto vulnerabilities.

A next line of inquiry is what asymmetric entities among existing terrorist organisations might become the first actor to use information weapons or to attack the vulnerabilities of modern information society?

This debate is unlikely to be settled soon as different schools of thought among the research community hold different arguments and empirical evidence. This paper seeks to illuminate the complexities in understanding a potential leap towards convergence and it offers a potential roadmap towards necessary measures to bolster investigative and enforcement mechanisms within the international community.

Before proceeding to the substance of the paper, it is necessary to focus on and clarify definitional aspects to set the parameters of this paper. The focus here is on advanced non-state actors who have both a motivation (and capability) to strike against National Critical Information Infrastructures. Critical Information Infrastructure Protection (CIIP) is the core of a broader concept encompassing Critical Infrastructure Protection (CIP), which, for the purposes of this paper can be further divided into five areas:

- Continuity of government. Defined as the information structure which supports the national decision-making processes and how it's communicated (television and radio broadcasting structures, etc.)
- The Power Sector
- The Telecom/ISP Sector
- The Financial Systems (mostly in private hands)
- The Air Traffic Control System (within the larger Transportation Sector).

The common denominator for all these aforementioned areas is that an attack against these may yield disastrous effects in milliseconds in comparison to a biological or chemical agent (the poisoning of a water reservoir), which can take hours or days to produce an effect.

Information-/Cyberterrorism – Fact or Fiction?

An underlying rationale for this paper to merge the field of terrorism studies within the realm of Information Operations (IO)[127] was to fundamentally question the relevance of the connection between traditional terrorism and cyber terrorism. In many ways one can liken this question to the parallel scholarly debate that existed in the 1970s and 80's attempt to connect the seemingly parallel universes of terrorism[128] and CBRN weapons. Most academics discounted

[127] Information operations (definition): *The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called IO.* (US DoD JP 3-13)

[128] Definitions on terms used by the author specifically for the purpose of this article derived from the Pollard/Devost-matrix on page 3.

Information-attack (means)
Attack or manipulating by using infologic, electromagnetic, cognitive or physical means in order to achieve a certain purpose.
Information Terrorism*
An act of terrorism conducted through information-attacks.
Cyber Terrorism*
An act of terrorism conducted using infologic means and methods.
*Terrorism is defined in accordance with the EC framework and is normally regarded as activities related to non-state actors and defined as below.
In order to be labeled acts of terrorism, crimes (such as homicide, manslaughter, kidnapping, sabotage etc.) should meet the following criteria:
1. The act should seriously risk damaging a state or an interstate organization.
2.The purpose with the act should be:
a) To inflict serious fear among population or sub-population, or

this possibility on the grounds that most terrorist groups were inherently conservative and had a built-in desire for cost-efficiency to rely on the bullet and the bomb due to its ready availability, organizational and financial reasons, national contexts and fear due to backlash from their own constituencies and states, as well as a lack of scientific expertise necessary to move in this direction.

In struggling to control the forces of globalization in an age of al-Qaeda and the proliferation of CBRN material, the conventional wisdom among security officials and academics has been to question *when rather than if* transnational terrorists will strike against a major western capital with the ultimate ”weapon of mass disruption.”

As CT expert Dr. Neal Pollard points out in an interview, both CBRN and Cyber/Electromagnetic-dimensions offer technological opportunities for terrorists to increase their capability, given such groups overcome technical hurdles and intent converges with capability. However, the pursuit of CBRN provides groups with additional risks and opportunities for interdiction by CT efforts, as cyber is pursued as both a tool and a weapon. In addition, increased effectiveness allows groups to deny opportunities for interdiction.[129]

The revolution in information technologies has opened up almost infinite constellations of possibilities in connecting the realm of post-modern terrorism with cyber terrorism.[130] In understanding the parameters of this scenario it is useful to divide the many components of information/cyber terrorism into a *critical infrastructure threat matrix*[131] to underscore the spectrum of combinations possible in attack mode and targeting on the physical or digital levels.

This critical infrastructure matrix illustrates that an attack could assume the form of either cyber terrorism, information terrorism or an information attack. In terms of definition, information attack (as a means) denotes “an attack or manipulation by using infologic, electromagnetic, cognitive or physical means in order to achieve a certain purpose.” Conversely, information terrorism is defined as “an act of terrorism conducted through information-attacks” and cyber terrorism denotes “an act of terrorism conducted using infologic means and methods.” As such, in this typology the wider term *information terrorism* includes multiple components and combination such as electronic warfare, kinetic attack, denial and deception, pure computer network attack, and the use

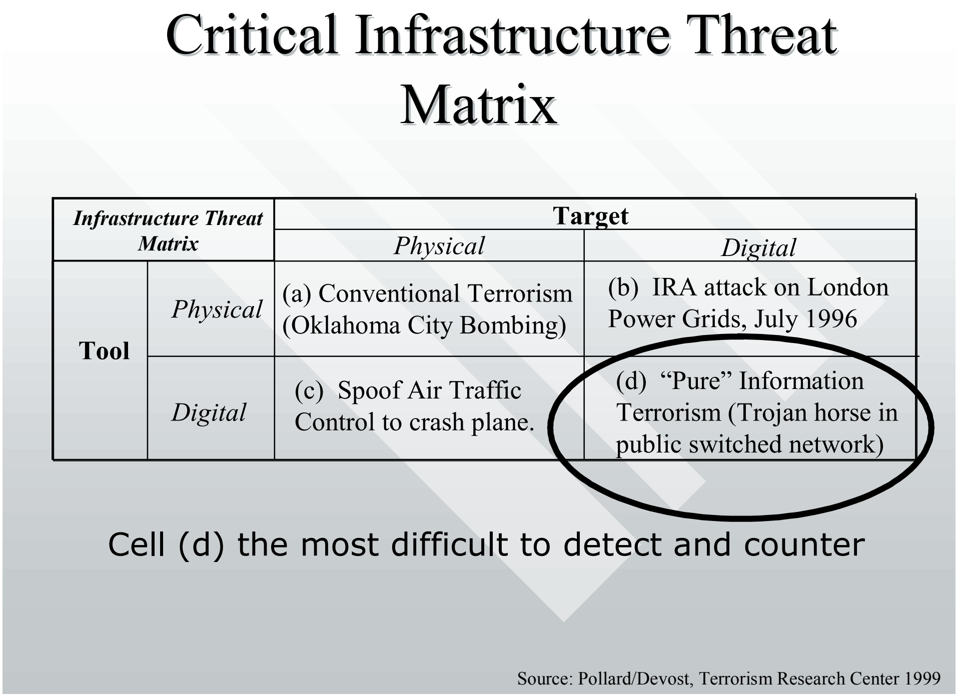
b) To blackmail public or interstate organizations to commit or not to commit to a certain behavior,

c) Seriously destabilize or destroy the critical political, constitutional, economic or social structures within a state or within an interstate actor.

[129] Interview with Neal Pollard (JD), adjunct professor at Georgetown University, on September 11, 2007

[130] See: John Arquilla, David Ronfeldt, and Michele Zanini, “Information-Age Terrorism”, *Current History,* April 2000: pp.179-185.

[131] Matt Devost and Neal Pollard, Terrorism Research Center, McLean, Va., originally developed this framework.



Critical Infrastructure Threat Matrix

Infrastructure Threat Matrix		**Target**	
		Physical	*Digital*
Tool	*Physical*	(a) Conventional Terrorism (Oklahoma City Bombing)	(b) IRA attack on London Power Grids, July 1996
	Digital	(c) Spoof Air Traffic Control to crash plane.	(d) “Pure” Information Terrorism (Trojan horse in public switched network)

Cell (d) the most difficult to detect and counter

Source: Pollard/Devost, Terrorism Research Center 1999

of more exotic technologies such as directed energy weapons or electromagnetic pulse weapons.

In regard to this threat matrix, the question remains - Is there a credible or even likely connection between terrorism and information/cyber terrorism beyond the vulnerability of our critical infrastructure? A major study in 1999 by the Center for the Study of Terrorism and Irregular Warfare (CSTIW) at the Naval Postgraduate School in Monterey, California, entitled *Cyberterror: Prospects and Implications,* concluded that the technological barriers were too high and that “terrorists lacked the human capital needed to mount a meaningful operation.”[132] Other studies have similarly concluded that cyber terrorism is unlikely to be a future threat and not an immediate issue. These assessments may have been realistic at the time, but suffered from methodological weaknesses as to the selection of the groups and understanding of the changing nature of terrorism itself.[133]

[132] Dorothy E. Denning, “Is Cyber Terror Next?” *Social Science Research Council/After Sept.11*

[133] In fairness to the Naval Postgraduate School, whose CSTIW scholars and academic work regularly provides the direction of cutting-edge research often many years ahead of others on a multitude of issues, the conference participants recognized the limitations of the study due to the limited sample of groups included. See: David Tucker, “The Future of Armed Resistance: Cyberterrorism? Mass Destruction”, Final Report on a Conference Held May 15-17, 2000 At The University Pantheon-Assas (Paris II).

Understanding the transformation of possibility into reality in the cyber terrorism realm requires an in-depth understanding of the relationship between motivation and capability. This convergence has been complicated not only by the phenomenon of al-Qaeda itself and the next generation of terrorists with new digital expertise and weapons, but also the fuzzy boundaries between crime and terrorism and the availability of free-lance advanced hacking and computer expertise. There are four principal examples that point towards a trend of increased convergence - though yet far from fully developed - between terrorism and information/cyber terrorism:

First, the Provisional Republican Army (PIRA) in Northern Ireland planned in July of 1996 to blow up six electric switching stations (pumping stations and gas plants outside the London security "ring of steel") as part of their Mainland terrorist campaign. In this foiled plot, the six-member cell had 37 explosive devices under construction, which would have caused serious cascading effects by disrupting the power supply of London for an extended period of time.[134] Furthermore, this had been preceded by a sustained PIRA campaign to use hoax calls to disrupt infrastructure services.

However, this incident is far from unique, as other terrorists have long targeted key components in the critical infrastructure elsewhere. In fact, the U.S. Department of Energy estimated in 1997 that saboteurs worldwide attacked over 20 000 electric power targets over the past ten years.[135] A majority of these incidents were not terrorist-related, though some were major terrorist/insurgent groups who have specialized in disrupting electricity pylons and substations as well as oil pipelines.

In March of 2000, a second major incident implicated Aum Shinrikyo when Japanese police discovered that software used to track 150 police vehicles had been developed by the cult and that they were in possession of classified tracking data on 115 police vehicles. Furthermore, the Aum cult (now renamed Aleph) owned computer software development companies that had developed software for at least 190 Japanese firms and 10 government agencies providing 210 different types of software systems.[136] Aum was so embedded that a member was involved in the development of the key command and control system of the Maritime Self-Defence Force – a system controlling information on the movements of warships and aircraft.[137]

A major fear spread that the Aum cult placed malicious codes into its software to allow remote access to facilitate attacks. Even a declassified CIA document submitted to a special Senate hearing in April 2002 identified the cult as

[134] See: Patricia Irwin, "How deregulation increases network vulnerability", *Electrical World,* October 1997.

[135] *Ibid.*

[136] "Defense Agency orders software-makers to be ID'd", *Mainichi Daily News,* May 16, 2000.

[137] "Cultist worked on MSDF system", *Asahi News Service,* April 14, 2000.

having the potential to mount a cyber terrorist attack on the United States.[138] These cyber capabilities were compounded by the fact that software developers of Aum had siphoned off information about Japan's nuclear programme, including nuclear fuel suppliers, research and transportation of nuclear materials while they had compiled an extensively detailed personnel information database of 75 researchers dealing with nuclear matters.[139]

These AUM-affiliated computer firms also earned the cult around $65 million per year through the sale of computers.[140] Even software, based on a game teaching math was developed and designed to attract high school students to the cult's apocalyptic theories about the end of the world.[141]

A third example is related to al-Qaeda's expertise in the cyber-domain both as an advanced intelligence tool and even displaying hacking expertise in terms of distance reconnaissance of critical infrastructure targets. As demonstrated by Dr. Magnus Ranstorp,[142] the matrix of Islamist fanatics underneath al-Qaeda's umbrella was extremely well versed in computer skills to enhance their C3I-capabilities.

Al-Qaeda also used Information Technology offensively. In a small al-Qaeda notebook found in a *Mujaheedin* training camp in Afghanistan in December 2001, an al-Qaeda reconnaissance team outlined their ability to retrieve a U.S. diplomat's movements by breaking into his e-mail account and retrieving his bank statements. In addition, al-Qaeda has also displayed an interest in carrying out reconnaissance on critical Supervisory Control and Data Acquisition (SCADA) systems inside the United States. This advanced cyber capability is expected not to diminish as the private sector has identified Pakistan, Iran, Egypt, and Indonesia (bordering Russia and China) as virtual hotbeds of information warfare and hacking talent.[143]

A fourth (and by no means final) example of increased terrorist interest in offensive cyber capabilities relates to the report issued by the Russian Federal Security Service (FSB) alleging that the Chechen field commander Khattab had a cell that specialised in efforts to hack into the computer systems of 10 major European banks towards the end of 2001. In this detailed plot, Khattab's cell sent out a skilfully forged commercial offer via e-mail from the Bank of Ireland

[138] "CIA said Japan's AUM cult poses cyberterror threat", *Japan Economic Newswire,* October 29, 2002.

[139] "Cult Siphoned Nuclear Data", *Asahi News Service,* March 29, 2000.

[140] Calvin Sims, "Japan Software Supplier Linked to Sect", *The New York Times,* March 2, 2000.

[141] "AUM computer firm used games software to lure new followers", *Mainichi Daily News,* April 25, 1995.

[142] Magnus Ranstorp, "The Virtual Sanctuary of al-Qaeda and terrorism in an age of globalization", in Johan Eriksson and Giampiero Giacomello, *International Relations and Security in the Digital Age* (Routledge, 2006).

[143] See: David Rennie, "U.S. warns of cyberwar threat to security", *The Daily Telegraph,* August 23, 2002.

with a highly advanced "Trojan horse" (Back Orifice). The complexity of the concealment was unique with "a triple-layer pseudopolymorphic shell."[144]

These converging trends in the direction of advanced hacking or cyber terrorism seem to indicate that these groups are more advanced than generally recognised and fall in between the capability categories of advanced-structured and complex-coordinated, developed by the Naval Postgraduate School's 1999 study on the prospects of terrorist organisations pursuing cyber terrorism.[145] This and other studies have not taken into account the potential for GPS-guided explosives[146] or even more exotic technologies harnessed by terrorists such as High-Energy-Radio-Frequency (HERF), Transient Electromagnetic Devices (TEDs) and Electro-Magnetic Pulse (EMP) weapons (suitcase type, "can-bombs" etc.) or the even more sophisticated Directed Energy Weapons (DEW). If, for example, an Airbus could be made to crash over Schipol airport by terrorists through a DEW/EMP-attack and be filmed by a TV-camera – or a cellular camera - it would naturally produce a 9/11-effect with dramatic human and societal consequences.

Some critics may argue that this scenario represents a distant future and improbable threat. And they may be right. However, any such probability assessment must be balanced against the availability of this type of technology for sale on the underground market place. The Swedish Defence Research Agency (FOI) discovered in 1998, a Russian suitcase bomb emitting short, high-energy microwaves. It was developed by a Russian Technical Institute and was for sale for $100.000 to any interested buyers.[147]

Similarly, TEDs can be built on a very low budget in a matter of weeks by someone with an electrical engineering background and, if hooked up to satellite-dish television antennas, be operated out of a minivan or a house. This methodology would reduce logistical footprints and could hypothetically bring down an airplane and damage different sectors of IT-dependent information systems.[148] Even a failed attempt, if disclosed in public could produce highly damaging psychological cascading effects.

These scenarios become even more menacing when one considers that EMP or Directed Energy Weapons (DEW) are part and parcel of the security threat matrix in NATO intelligence briefings, though it is unknown whether the terrorists would possess the technical expertise to launch such an attack.

[144] "Chechen rebels trying to hack into European bank accounts", *Izvestiya,* September 18, 2002.

[145] For further discussion of these categories, see: Dorothy Denning, Cyberwarriors: Activists and terrorists turn to cyberspace, *Harvard International Review,* Summer 2001, Vol. 23, No. 2; Pg. 70-75

[146] In 1995, Dr. Magnus Ranstorp teamed up with two other academic colleagues with physics background and developed a study in two weeks on the potential for GPS-guided terrorist weapons. This study was never published for security reasons and on the advice from military officials.

[147] See*: Svenska Dagbladet,* January 23, 1998.

[148] James P. Lucier, "E-Zapper could break the bank", *Insight on the News,* May 25, 1998.

It is expected that any deployment of EMP would occur in conjunction with a kinetic attack.

Perhaps this worst-case catastrophic scenario will hopefully never develop nor materialize in the near future. But consider the ease to which it is possible to harness a wealth of publicly available open-source information in cyberspace that exposes vulnerabilities in any state's critical infrastructure protection. A prominent case in hand of the power of open-source intelligence is Sean Gorman's PhD research at George Mason University that single-handedly mapped out America's fibre-optic system and the layered connections to every business and industrial sector of the economy. In Gorman's case, Richard Clarke, the White House cyber terrorism chief, underscored the national security concerns by advising that "he should turn it in to his professor, get his grade – and then they should burn it." [149]

For terrorists, cyberspace has emerged as a force-multiplier in intelligence gathering and target-acquisition from afar. Equally, the availability of commercial imaging satellite products to global citizens illustrates the changing dimensions of information and security, enabling terrorist groups to have a global intelligence capability – even from space.[150] The critical ingredient both for the intelligence analysts and the terrorists is not to gather information in today's networked society and increasingly borderless world, but to transform it into a weapon of knowledge. As such, mapping and assessing this process of transforming information into knowledge, inside the inner vortex of a terrorist group's compartmentalized decision-making process is more difficult than ever, especially with the potential to harness cyberspace as an offensive weapon.

It goes far beyond categorizing terrorist groups into simply following the principle of "the path of least resistance," especially when considering the amplifying effects of cyber-attacks in conjunction with a kinetic attack. Just as the bomb designer is more critical for a terrorist group than a bomb maker, it is necessary to contemplate the almost infinite recruitment possibilities of terrorists of IT specialists through moles inside corporate and government organizations, free-lance politicized hackers, or even state-sponsored cyber terrorism.[151]

The blurring boundaries between terrorism (politically/religiously motivated) and crime (economically motivated), both ordinary and organized across the globe make this scenario even more probable and difficult to detect and control, especially as cyberspace affords a high degree of anonymity for both criminals and terrorists.[152] How does one detect the identity of a cyber-attack at the other end and how does one respond in real-time if the cyber intrusion is routed through multiple countries?

[149] For details, see: "The cybercommando", *Vancouver Sun,* July 19, 2003.

[150] "Private eyes in the sky", *The Economist,* May 6, 2000.

[151] See: Eric D. Shaw, "A Limit to Cyberrteror", *Information Security,* September 2002.

[152] According to Mi2g, Brazil tops the list of countries with hackers and criminals in the cybersphere, see: Tony Smith, "Cybercrime's superlab: Brazil", *International Herald Tribune,* October 29, 2003.

This potential situation is even more complex when one considers that the distinction between military and civilian targets will blur in future conflicts, especially as the latter civilian commercial entities are extremely reluctant to report any intrusions and attacks due to negative effects on consumer confidence and potential economic losses. The cost of losses from and protection against these threats are staggering in scale and scope.

The worldwide collective economic damage from overt and covert digital attacks during 2006 is estimated at $52 billion.[153] The rising transnational connections between digital "warriors" and their rising sophistication in attack mode, have contributed to CEO's and board-makers within S&P500 and FTSE-100 companies seriously contemplating insurance against a $100 billion global cyber catastrophe.[154]

Here one could ask if companies are doing enough, and in particular if the insurance industry is paying enough attention to the risks involved. The insurance industry could be the key to foster a better due diligence culture within the whole private sector. Especially in Europe, the insurance companies remain very conservative and reactive - they do not bother "as it has not happened yet."

The issue of increased vulnerability of critical infrastructure from the potential consequences of a revolution in information technology is not a new one. Back in 1997, the U.S. National Security Agency (NSA) simulated a terrorist attack with 35 terrorists, who managed to hack into "Department of Defense networks, 'turn-off' sections of the power grid, 'shut down' parts of the 911 emergency service."[155]

In more recent times, an array of simulation exercises such as DPH (Digital Pearl Harbor) by the U.S. Naval War College; SECTOR5 (Summit Exploring Cyber Terrorism); and a host of other national and international forums have underscored our inherent collective vulnerabilities. More recently in the post 9/11 environment, security officials worry about the change in discourse within al-Qaeda's leadership, emphasizing the intent to cause massive financial disruption over the desire to cause human casualties.[156]

Most terrorist groups today have long seized on the opportunities accorded by the information revolution through an established multiple web presence. This is especially true as they have gained access to a platform for uncensored propaganda for skilful perception management. IT is an ideal auxiliary recruitment tool for reaching out to an infinite audience and talent pool of potential recruits and as a new form of auxiliary fundraising.[157] Some of these terrorist

[153] CSI/FBI Computer Crime and Security Survey, Computer Security Institute 2006

[154] See press release at Mi2g website at www.mi2g.com.

[155] Dickon Ross, "Electronic Pearl Harbour: Should we be more worried about terrorists using digital weapons rather than chemical and biological attacks." *The Guardian,* February 20, 2003.

[156] Dan Verton, "Experts: Don't dismiss cyberattack warning", *Computerworld,* November 18, 2002.

[157] Among the best sources for the modalities of terrorists' use of cyberspace is the col-

groups have been engaged in quite advanced forms of ”e-jihad” against their enemies, providing a virtual dimension to their fighting on the ground. What is much less obvious in many cases is hard evidence of how far down the road they have gone in seriously investigating the potential use of cyber space as an offensive instrument.

One underpinning overall assumption in this context is that terrorists groups and qualified non-state actors such as al-Qaeda are moving up the ladder of the “learning curve.” Mortar techniques proliferated from PIRA in Ireland to the FARC guerrilla in 2001, due to a “mobile training team,” which quite soon resulted in raising the effectiveness of FARC attacks against the Colombian troops[158]. Another more recent example is the spreading of IED techniques from the insurgency in Iraq to Afghanistan and other locations. The Internet is further enhancing the speed of the terrorists’ destructive knowledge.

Thus, it is not from a “mathematic-logic” standpoint inevitable that information terrorism as described will occur. However it does not seem like an unnatural path for qualified non-state actors to move in this direction in the future. Consequently, the combination of these factors means that nations cannot afford to ignore these developments.

Conclusion

What To Do? – Some Recommendations

If these concerns described earlier are not to be dismissed, what can governments and the international community do to counter this spectrum of threats? It seems also that the one-year timeframe for executing information terrorism seems more likely than the ten-year view according to the previous discussion. Hence, according to the author’s view there are three issues that need attention:

Whose laws apply?

On January 19, 1999, the website of the East Timor-movement (the ”.tp”-domain) based on a server in the Irish Republic was “shot down” with a DDOS-attack.[159] The host of the server, Connect Ireland, suspected the Indonesian State Intelligence Service and filed a lawsuit against the Indonesian government. It is unclear who was responsible as it later “faded away” and no action was taken or reported. A principal problem underscored with this example is what kind of law applies in this situation? Is it the Irish law as it concerns the integrity of the Republic? Or is it a civil law case and “a matter of “due diligence.” If this attack was routed through other countries and violated their cyberspace, what are the legal consequences or have they not yet been anticipated?

lection of essays in Russell D. Howard and Reid L. Sawyer (eds.), *Terrorism and Counterterrorism: Understanding the new Security Environment* (McGraw Hill, 2004).

[158] http://www.ncjrs.gov/pdffiles1/nij/grants/208552.pdf , R. Kim Cragin ... [et al.] “Sharing the dragon’s teeth: terrorist groups and the exchange of new technologies” MG-485, RAND Corporation, 2007, p. 84

[159] http://news.bbc.co.uk/1/hi/sci/tech/263169.stm

If an attack is politically motivated on the sender's side it will still probably appear as a criminal act at the receiver's end. Thus, there is generally a wide gap between the intent behind the act and the laws to counter those acts on the other end. i. e. the laws not updated for this kind of sovereignty breaches in the Information Age.

Need for regimes and Rules of Engagement (ROE) for Law Enforcement Agencies to be able to trace back in near real-time.

One issue on the defensive side of international co-operation is the need for improving the possibilities of making "trace-backs" in near real-time. If an attack on a Swedish information system originates in another country, it would take several days for the subject of the attack, e.g. a telecom operator, to learn more about the whereabouts of the perpetrator. They would have to contact the Swedish police, who in turn would make contact with the police in the country from which the attack had come and request assistance from the telecom operators concerned in that country. Therefore, it is important for Sweden to provide active support for international agreements and regulations designed to facilitate rapid tracing across national borders. In the latter case, the relevant G-8 committee has produced recommendations in this direction with the endorsement of the Council of Europe.

At the 53rd meeting of the United Nations General Assembly in December 1998, a resolution (UNGA 53/70) proposed by Russia was – after some modifications from US and other countries - unanimously adopted to the effect that the threat to civil information systems, for example from terrorists and criminal groups, should be heeded by the international community and cross-border measures should be implemented. In the continuing discussion on this topic prior to following year's General Assembly, the need for bilateral as well as multilateral (UN, Interpol) contacts emerged.

There is a proposal called the "Stanford Treaty" which appeared in the year 2000 from the former legal adviser to the Reagan administration, Abraham Sofaer from Stanford University and Sy Goodman from Georgia Tech[160], which made a reference to the hijacking problem within the airline industry in the 1970s. The way to reduce the scale and scope of this problem was through a UN-resolution, which created a universal treaty, and every state that wanted an international carrier to land on their airports had to comply with the new safety and security procedures regulated in this treaty. To implement and audit this scheme a small "watchdog," the International Civil Aviation Organisation (ICAO), was set up under a UN mandate, and the problem was drastically reduced over time. Could a parallel procedure or body be established for oversight of cyberspace violations?

[160] Abraham D. Sofaer and Seymor E.Goodman: A proposal for an International Convention on Cyber Crime and Terrorism, Center for international Security and Cooperation, Institute for International Studies, Stanford University, August 2000.

The Stanford Treaty advocates a similar kind of treaty with an oversight body to create a universal mandate (UN or the International Telecom Union in Geneva) as the more security related closed relationship between certain countries ("five-eyes" etc.) do not have the necessary outreach to all 192-plus countries. The international community has to deny "safe havens" for rogue actors everywhere. If some countries, in for example the sub-Saharan region, do not have the available means on their own to have enough Information Assurance in the Telecom/ISP networks, maybe the World Bank or the International Monetary Fund could support them to raise the security bar. With such a treaty combined with an oversight body, it might be possible to start discussions on Rules of Engagement for near real time trace backs in other states' telespace. This would be a real enhancement of "collective security" in cyberspace.

Better watch-systems and CT-approach

In an insightful and comprehensive White Paper from Naval Postgraduate School in October 1999 some military students under supervision of Dr. John Arquilla analysed in depth the means, motives and probabilities for different terrorist organisations to be successful in going the cyber terrorism path[161]. Here was also a list of different activities that could serves as Early Warning indicators for the IC and CT-authorities. What needs to be added here is the dimension of Electro Magnetic Weapons. A need to watch for "trial and terror" patterns on training with digital or electro-magnetic weapons, or reconnaissance actions by terrorist suspects against air traffic control systems, or other vital national information infrastructures should be carefully logged. Any proliferation noted of Directed Energy Weapons (DEW) techniques should also immediately raise concerns.

[161] US Naval Postgraduate School, White Paper, Center for Irregular Warfare and Terrorism, "Cyberterror: Prospects and Implications", Monterey, Ca., October 1999; p. 114-115

Article 4

The Trojan Horse in the Information Age

First published 2006 in
COUNTERING TERRORISM AND WMD
by Routledge[162]
(Ed. Peter Katona, John P Sullivan, Michael D Intriligator)

[162] This text was to a large extent previously published in *Axess* no 5, 2002.

When the husband and wife futurologists Alvin and Heidi Toffler described the conflicts in the Third Wave – the Information Age – in War and AntiWar (1993) they argued that while the aims of a war or military campaign had not changed, the method of waging it had. A new form of warfare – Information Warfare – with a whole new doctrine had seen the light of day.

This change can be described in a simplified way as the difference between the theory of the nineteenth-century German strategist Clausewitz (that "war is merely a continuation of politics with different means", and that, consequently, war and peace are two clearly distinguishable conditions), and the theory of the Chinese strategist Sun Tzu (500 BC that "the highest art of war is not to win a battle but to win without battle").

In the latter case, the boundaries between peace, crisis and war are dissolved. It is a matter of retaining "the monopoly on formulating the problem", of getting one's adversary to behave as one wishes, perhaps primarily by influencing his will, but if this fails one must also be able to threaten and meet his objective capacity in a credible way.

What, then, are information operations and information warfare? In 1998 in the United States, the original concept of information warfare (IW) was given the new designation of information operations (IO), primarily because the private sector and civil authorities did not want to talk about warfare in peacetime. IW was then given the more limited meaning as "information operations during crisis and war" and primarily within a military framework. Like NATO, Sweden has adopted this change; the most semi-official definition can be found in the Swedish government's information technology bill of March 2000 (1999/2000:86, p. 36):

> Information operations are combined and coordinated measures in peace, crisis and war to support political or military goals by influencing or exploiting the information and information systems of the adversary or other foreign player. This can occur by using one's own information and information systems while these assets must also be protected. An important element is the attempt to influence decision-making processes and decision-making.
>
> There are both offensive and defensive information operations. These are carried out in political, economic and military contexts. Examples of information operations include information warfare, mass-media manipulation, psychological warfare and intelligence operations.
>
> Defensive information operations are coordinated and integrated measures in times of peace, crisis and war as regards policy, operations, personnel and technology to protect and defend information, information systems and the ability to make rational decisions.

Other closely related concepts are also used to describe partial methods of information operations. "Overarching information security" – also including policy, organisation etc. - is the IT-based defensive component and is collectively termed Information Assurance (IA). Perception Management is the cognitive form of exerting an influence, with psychological operations ("PSYOPS") as its most organised sub-category. In the context of civil preparedness, there is much talk of Critical Infrastructure Protection (CIP). Within the Swedish Armed Forces, the current reorganisation into a network-based defence (NBD) represents a new way of leading military units in which information can be converted into armed response, almost in real time. (

The most spectacular sub-category of information operations is offensive computer network attacks (CNA) in which info logic weapons such as computer viruses, Trojan horses, logical bombs and denial-of-service attacks attempt to attack specific information systems. Likewise, electromagnetic pulse (EMP) and high power microwave (HPM) weapons – for instance hidden in a briefcase – can without smoke, sound, light or smell, knock out or (at close range) even melt the electronics in vital information systems.

~

The effect, which such attacks could have on such targets as financial systems, has led official Russian representatives to draw comparisons with nuclear war and demands from nations, such as the US, that these systems should be included in arms control. The use of military computer network attacks should also require the same high decision-making level as the use of nuclear weapons. The comparison with nuclear war, however, falters in one important respect; since nuclear war was "threshold raising" in that both superpowers had a mutual, destructive second-strike capacity – the so-called balance of terror.

Today, when the "enemy" exists not only in one direction and conflicts are more multifaceted, with military, economic and religious elements, the anonymity involved in computer network attacks becomes "threshold lowering". How can a state retaliate if it cannot clearly identify the sender? On the other hand, what might someone be capable of doing, even against one's best friend, if there was no risk of discovery?

The other "sensitive" extreme in the spectrum of information operations is psychological operations with media manipulation and perception attacks. In the Western society with its strong media institutions it is almost anathema to assert that states should in some way use these methods other than at a relatively low military level.

The fact that Sweden's total defence approach provides this country with an agency, which in peacetime makes plans for psychological defence – though only in the event of crisis and war – arouses a delight mingled with terror among the defence planners of other nations. In the US, CNN and other institutions would start talking about a "Big Brother" society if the media there felt themselves likely to be influenced by a similar institution in any formal sense.

A proposal last autumn (2001) to create a special authority within the Pentagon to shape the strategic media image also had to be withdrawn after a media backlash. At the same time, the technical possibilities of virtual image manipulation (morphing) are almost unlimited, something, which can be seen in the Hollywood, films *Forrest Gump* and *Wag the Dog*. Since "seeing is believing", this can be a very effective weapon. The TV pictures showing hostages being executed in Iraq is also a very powerful message. The increased role of PR agencies in creating public sentiment, above all in third-party countries, in favour of one side of a conflict, by such methods as planting video sequences in news programmes was manifested at the start of the conflict in Bosnia. Representatives of the Serbs in Bosnia employed the Saatchi & Saatchi agency, while the Muslim side had their own PR firm. If in a corresponding way (for example during a crisis situation in the Middle East) a morphed video sequence were to be shown in which Israeli units were apparently bombing and burning down Mecca, this could have instant and irreversible effects on events before there would be time to make any denials.

A BBC Panorama programme, aired on April Fools' Day in 1963, purported to show the "spaghetti harvest" in Italy. The scenes of elderly Italian ladies sweeping soggy spaghetti into wicker baskets might have been faintly ridiculous but many people were convinced!

Particularly in peacetime, perception management and psychological operations are, like the intelligence services, "an extremely forbidden necessity" for the strategist who wishes to succeed. The line drawn between these methods and general diplomacy and politics can become blurred, as can the same line drawn vis-à-vis economic contexts, in which false press releases, the spreading of rumours, etc. can have a manipulated speculative effect on stock markets. This fact means that it is as important to be aware of, and have the means to discover and check, the sources of such information as it is to have hacker-detection systems and firewalls in computer networks.

~

To sum up, information operations are characterised by the fact that there are no demarcation lines regarding their use in the scale of conflict made up by peace, crisis and war. These operations can be implemented in political, economic and military contexts. There is always a strategic purpose even if implemented at a low level within an organisation. This means that an information operation must have the support of, and be synchronised at, the highest possible level: for a state at the highest security policy level, and for a company in the CEO's immediate circles. We cannot make a distinction between offensive and defensive expertise and capability: if you have one, then you have the other. The weapons can be cognitive, infologic, electromagnetic and kinetic; it is the purpose that is the decisive factor.

The asymmetry which characterises terrorism – it is no longer merely states which threaten states but also separate individuals/groups (e.g. bin Laden vs. the US) – is even more obvious in the field of information operations, since a single individual can theoretically cause serious IT attacks which affect important societal infrastructures. The media's role and what is known as "the CNN effect" reinforce this asymmetrical element. How much was the effect of the events of September 11th magnified by the fact that we could from early on and repeatedly with our own eyes follow the course of events and see the planes explode into the two towers of the World Trade Center? Would it have been equally traumatic if we had only heard about the event?

In the light of this, a crucial question has been how we can define the civil-military relationship in order to map out the relationships of responsibility within the civil services of different countries. One first important decision for the majority of defence forces in the mid-1990s was to define what was then called information warfare as either an operational- or an intelligence-oriented matter.

The Swedish armed forces, like the US and Germany, chose to regard this as an operational matter, i.e. as a weapons system, which a nation should be able to use in the same way as, for example, tanks and an air force to protect the country and ensure its survival. Others, including France and the UK, regarded the issue more as an intelligence matter. Consequently, completely different systems came to govern developments and influence what could be openly discussed. This has contributed to the fact that the EU has difficulty in addressing these issues. Even within NATO the discussion is limited because of differing national agendas.

~

To put it simply, based upon what the Swedish authorities have already published, we can talk about the following four dimensions of information warfare:

Defensive information warfare (IW-D), in which primarily the armed forces adopt measures even in peacetime to protect their own systems in the event of crisis and war. All countries talk about this.

Offensive information warfare (IW-O), in which the armed forces during crisis and war must have knowledge of such methods to uphold the nation's sovereignty and survival. Only a few nations have spoken openly about this: the US, Germany and Switzerland.

Defensive information operations (IO-D) can be regarded as a "total defence in cyberspace". Since this can also occur in peacetime, as well as in times of crisis and war, it is an issue for the national authorities in which the armed forces can only play a supporting role. It is perhaps only Switzerland and, in some cases, the US – though not when it comes to psychological defence – who openly declare their ambitions in this field.

Offensive information operations (IO-O) represent the most sensitive of these four dimensions and for which state authorities are unwilling to comment publicly since these are best classified as skilled intelligence operations.

Since the threat against national infrastructures has nevertheless been observed in all nations, particularly after September 11th, the term Critical Infrastructure Protection (CIP) has become the concept which most closely corresponds to IO-D, and which is used to denote protection against this kind of civilian threat. In recent years most Western nations have seen the construction of new cross-sectoral management structures to better handle the necessary cross-sectoral problems.

Thanks to the legacy of its “total defence system”, Sweden has an advantage that has not been fully exploited. This concept demands a highly holistic approach in the preparedness of both civil and military organisations in Sweden as the only way in which a small country might have any real opportunity of withstanding an attack from a much more powerful adversary.. In addition to military defence, the system encompasses an integrated defence against economic, psychological, security and infrastructural threats. Even in peacetime, the different sectors of society, both government and private, have been required to look towards this overall defence goal.

The problem with this model is that it is not intended to operate during peacetime and only come into effect in the event of national crisis or war. We are now faced with potential attacks which can occur at any time, and most likely in times of peace. This leaves room for conflicts of expertise (and interests) between different sectors – a situation which paralyses and delays objectivity and the necessary organisational, structural and operational changes. Sweden is still investing approximately SEK 40 billion in military defence, without knowing if we can, or are allowed to use such vital resources for peacetime non-military threats. It is imperative that we do not “throw the baby out with the bath-water”, but rather try to retain the holistic approach that characterised Sweden’s highly agile and successful total defence legacy, by developing new peacetime structures.

Within the defence establishment, information warfare has caused some perplexity and anxiety, particularly when it comes to the fundamental axioms of military theory. Firstly, the boundaries between tactical, operational and strategic levels are becoming increasingly blurred.[163] If a leaflet, supplied by a military PSYOPS-platoon within the SFOR force in Bosnia, comes under the cameras of CNN and ends up on the desk of the American President, it is definitely no longer a tactical issue. A tactical manoeuvre by units against an important network or telecommunications node must be synchronised at the highest level so that the effects do not exceed the intended ones (“cascading effects”), and, at the same time, not reveal or impede its own intelligence capability. Secondly, it has been discussed whether the Swedish philosophy of military leadership with its emphasis on assignment control has been a hindrance.[164] This leadership philosophy has been a hallmark of delegated deci-

[163] Tactical measures involve direct battle planning in near time (hours–days); operational planning occurs at the higher levels of staff and concerns the entire geographical area of operations with a longer time perspective (days–weeks); whilst strategic planning occurs at the national headquarters and Ministry of Defence level (months–years).

[164] Assignment control means that subordinate commanders can fairly freely solve the tasks given them by superior commanders with the allocated resources and with few other rules of conduct. Command and control involves control in detail.

sion-making ("auftragstaktik") within most of the Swedish armed forces, but is less well suited to these contexts, since very strict command and control procedures are the only possible way of managing IO/IW during the early stages of conflict, which is when information warfare is most effective.

What, then, does the threat scenario look like today? The traditional formula of intelligence analysis, "Threat = Intentions × Resources", should in the Information Age be expanded to "Threat = Intentions × Resources × Vulnerability". A country with heavy IT dependency (like the United States) is naturally more vulnerable than an underdeveloped country that lacks societal IT structures (such as Somalia). On the side of the perpetrators, distinction should similarly be made between states, terrorists, criminals and individuals (hackers).

One basic difficulty for a defender is to reliably know the identity of the attacker in the event that this is concealed or that the address is false (spoofed). Despite bold rhetoric about hitting back, it can be hard to guarantee that one is not actually attacking a hospital and putting vital life-support systems out of action. Which state department takes responsibility is often confused and can lead to delays in launching an effective response: if the attacker is a nation state, it would be the job of the armed forces; if, however, the attacker is a criminal or a terrorist, it would be the business of the police. But how do we know? Before we have figured it out, the question has probably become obsolete….

When it comes to individual countries, the US has the largest – and openly acknowledged – military capability in this area, but even nations like China are investing a lot in both doctrinal and structural development, setting up a special reservist organisation for information warfare. A semi-official treatise, Unrestricted Warfare (1999), written by two Chinese colonels described the intention to use both "soft" PSYOPS methods and "hard" network attacks against, above all, the US. The aim was to particularly exploit the United States' Achilles heel in the form of the population's low tolerance for casualties: for example, it was believed that a terrorist attack against a military base with a resulting large number of dead soldiers would create pressure on the American government to withdraw from most conflicts which do not affect the American homeland. In many other countries, information operations are regarded as an intelligence matter and not as operational, which limits the amount of public knowledge.

We have not yet seen many cyber-attacks launched by terrorist groups. In a 1996 paper, Dr. Andrew Rathmell of King's College, London, compared the willingness of the Muslim organisation Hamas and the IRA to use infrastructural attacks and IT weapons. He found that the IRA had sent people from their attack units on computer courses and had located crucial electricity nodes in London for a coordinated attack against commerce and the economy. Yet they had desisted. Why? His conclusion was that within traditional terrorist structures like the IRA, with its hierarchical organisation and its blue-collar leadership, there existed a greater resistance to using these methods despite their effectiveness – they wanted things to go "bang". In contrast, Hamas, with its academic leadership and its network-oriented organisation might be more inclined to use cyber-weapons and infrastructure attacks.

Al-Qaida has begun to use IT methods to communicate secretly, but there are examples of more offensive use. In the tapes used for internal training found in Afghanistan 2002 signs of Intelligence Preparation of the Battlefield (IPB) were found for attacks on major power grids, dams etc in western USA.

The AUM sect in Japan, in addition to using poison gas in the Tokyo underground system, was also involved in developing both biological weapons and manipulating the software of government information systems. It turned out that a software company controlled by the sect had been responsible for programming the positioning system, which the Japanese police used for their vehicles and police officers. The sect probably knew exactly where the police were at any given moment.

A most crucial question today is when the trend of exploring infologic and electromagnetic methods or/and aiming for infologic and information infrastructure targets on one hand, will transform to execution of real attacks with high amplitudes. It is no longer a question of "if"– it's about "when", but is it within one year, five years or ten years? Some otherwise conservative security services have estimated the shorter term here.

A scenario could be if some terrorists with HPM-weapons could disturb the Air Traffic Control on the ground or the wireless flight data hubs inside the airplane. If you got an Airbus to crash over Los Angeles or Amsterdam with 400 causalities ***and*** on the same time had a TV-camera - or an new cellular with a camera – sending out images of that catastrophe from ground, I would argue that this would create a 9/11-effect.

When it comes to serious crime involving IT elements, there are not many publicly acknowledged examples because it is in the very nature of this crime that the number of unrecorded cases is very high. There is only one known computer attack against a financial institution – against Citibank in 1994 when the Russian leader of a qualified hacker group, Vladimir Levin in St. Petersburg, succeeded in extracting $400,000 – but he had been close to getting $70 million. Citibank reported the crime to the FBI, upon which Citibank's competitors announced to their own customers and the world: "We haven't had that problem." The immediate effect was that Citibank's four largest customers withdrew about $1 billion each. The incentive for companies to talk about similar events since then has not increased, even if rumours of successful computer-based coups and extortion against banks is occurring with much greater frequency.

When it comes to individual hackers, the most expensive attack to date was the "Love" virus in Spring 2000. Originating in Manila in the Philippines, this virus caused damage worth an estimated $90 billion to information systems around the world. In Sweden we were helped by the time factor, even though the airline SAS and others suffered. Asian companies discovered the virus first; American anti-virus companies then had the night in which to find countermeasures, which Swedish companies could then use before booting up their systems in the morning. A number of IT security experts and administrators pointed out at the time that if this was what two young people could do in five hours, what might a nation achieve with specially targeted viruses or by releasing some kind of mass virus close to the intended target?

How, then, should we view IT weapons? Can they be a force for good, in the hands of the democracies or are they always likely to be the weapon of choice of the "bad guys"? As with all weapons, they are merely tools for the conduct of international affairs and these weapons will mirror the purposes for which they are launched. One major problem for the international community is the ability to intervene in international conflicts before they escalate to an unmanageable level. At the same time, more and more countries are concerned about their own losses in such conflicts. The American hesitation to send ground troops to the Balkans is one example of this. Thus, demand has recently arisen for a more flexible "toolbox" with more alternatives than the traditional military use of force using, for example, "smart sanctions" and conflict-prevention measures.

An article by an American military lawyer drew attention to Article 41 of the UN Charter, which proposes breaking off postal links and telecommunications with the aim of maintaining international sanctions. He constructed a scenario involving an application of IT weapons in accordance with Article 41 to maintain (what were in reality ineffective) sanctions against Rhodesia in the 1960s.

In this scenario, a unit would be able to identify, by means of a needs analysis, critical telecommunications nodes and knock them out. This would result in major communications blackouts, which would effectively maintain the sanctions. This action would be done within the broader concept of "use of force" and not within the narrower (and harder to decide on) "use of armed force". Even in the case of other international interventions, there would probably be a need for the UN-appointed military commander to have a more flexible toolbox.

Humanitarian aspects also indicate the need for an overhaul of international law. In a conflict involving an internationally sanctioned intervention such as the one in Kosovo in 1999, it is currently in accordance with international law to bomb a bridge on which there is a military truck even if twenty civilians also on the bridge are killed. In contrast, it is probably in conflict with the current interpretation of international law to cut off a civilian telephone line in the same area, even if that would have had a far greater effect on the war efforts of the Milosevic regime. International law and the laws of war are still based to a great extent on the legacy of experiences from the Napoleonic wars and are thus scarcely suited to the Information Age. The issue will be how the UN can develop broader Rules of Engagement (ROE) that can be implemented through the national command structures of individual nations.

~

To sum up, in the light of possible conflicts and threats in the Information Age, we can perceive changes in four important dimensions. Firstly, there is no longer any very clear difference between public and private dependencies. Reciprocal dependencies are at stake; and here the realisation that the state bears a responsibility for the commercial infrastructure must have an effect. The state had no formal responsibility for the banks during the crisis of the Swedish krona in 1991, but there was no other authority that could take the responsibility, and the state's role as "insurer of the last resort" then became obvious even in Sweden. Since such situations cannot be ruled out, we must also be able to plan for them.

From an Information Assurance standpoint the role of the Insurance and Reassurance Industry is crucial. If we can get their active involvement in developing insurances for the new risks - - with low probability but with huge consequences and thus no actuary data – we could promote more sound Risk Management procedures within the private sector. When the costs for vital IA-measures reach the CEO-level instead of the CIO within a company, the foundation of the critical infrastructures would be much safer and reliable. It will be a self-regulating mechanism based on market values and incentives. That also implies that the role of government – with the taxpayers money - only need to support measures for strengthening the private sector against effects that are beyond the business optimum, or where the knowledge of those threats primarily is out of bound for the private sector and more of a government issue for the Intelligence Community.

The role of Information Sharing is also critical. When it comes to develop Private Public Partnerships and the necessity of creating Information Sharing Analysis Centers (ISAC), there should be an impartial broker ("priest") to whom the companies with trust can perform their "confessions". This is according to my view the reason why Global Integrity had such a success running the financial ISAC, compared to some others where different industrial associations are in charge. In the latter category there are often a sense that one's competitor would take gain of vulnerabilities which reduces the willingness to share.

Secondly, the relationship between civil and military authorities has changed. "During the Cold War, the civil defence was supposed to support the military defence – now it is the reverse." This statement was made by the former Norwegian Prime Minister, Kåre Willoch, who some years ago headed the Vulnerability Committee specially appointed by the Norwegian parliament. The final report contained demands for major structural changes to the Norwegian political establishment. In Sweden we have so far been hampered by what is known as "the Ådalen syndrome",[165] which has maintained a very strict regulatory framework when it comes to the use of military resources (c.f. Posse Comitatus). In 2003, however, a new committee of inquiry suggested that it must become easier to use these resources on the condition that the use of force was excluded.

Thirdly, it is no longer possible to rely on any division of the conditions of peace, crisis and war when it comes to the relationships of responsibility for meeting the new threats. Flexible coordination between the police and the military must be established similar to that of the US, whose new Department of Homeland Security appears to have an increasingly strong mandate. In Sweden, for example, a civilian (police) command should be able to request the NBC unit which is currently being built up within the Swedish Armed Forces to handle this kind of terrorist event.[166] Training of these cross functional groups will require priority.

Fourthly, there are no borders in cyberspace. Since the link between grand strategy and the economy has become increasingly strong, threats, in particular anonymous IT attacks from other nations, can occur against economic players in another country. International security measures must therefore be developed by means of collaboration between as many countries as possible and at all levels. Legal and technological regulations must be harmonised so that a cyber-attack can be traced and stopped almost in real time.

It is impossible to make any distinction between offensive and defensive "capability". It is only the hard-to-access "motives" which can provide guidance. Since technological equipment is extremely useful for both peaceful and antagonistic purposes ("dual-use"), so in principle every young computer "geek" can, with completely legitimate motives, acquire the necessary equipment. This means that demands for arms control in the IT sphere are no longer applicable and that prospective enemies must be identified from a far larger arena than has previously been the case.

The realisation that cross-sector threats demand cross-sector solutions must also influence the design of any national defence strategy in the field of information operations.

The dramatically increased need for a rapid connection between "threat" and "planning" can – if the will exists – be handled within our Swedish system. A first step has been taken with the establishment of the Swedish Emergency Management Agency, but further changes are also needed to overcome the stovepipe structure of government and achieve a more horizontal, layered structure. This is as much a cultural issue as it is one of technology. Changes

[165] In 1931 a strike in the district of Ådalen led to battles between the demonstrators and military forces in which five civilians were killed and five wounded. One result was the establishment of a national police force and a ban on the use of the armed forces against Swedish civilians. (Ed. Note).

[166] The NBC unit is a military unit, which will be established to handle (limited) attacks involving nuclear/radiological, biological and chemical weapons.

can and should be developed through the collaboration of civilian, military and police authorities and, above all, in conjunction with the private sector.

Article 5.1

The role of Think Tanks in the US Security Policy Environment: A Forgotten Actor?

Published 2015 in
International Journal of Intelligence and Counterintelligence
(Vol. 28, No. 3, May 2015, 480-501)
by Routledge

Abstract

This paper seeks to explore if and how think tanks (TTs) influence the policy process. On the one hand there are theoretical explanations that have been offered by the academic community, which is a hot and varied debate. On the other hand, is how practitioners view the issue. A theoretical overview is provided, which is complemented by the distribution of a questionnaire to experienced practitioners. The United States is chosen as the case study, and a questionnaire was circulated among experienced and senior practitioners. Think tanks often set about creating their own opportunities to influence the policy process. The ability to exert an effect is influenced not only by what they do, but also the reputation and brand of the organisation. Five think tanks emerged, among the opinion of the experts, as the most influential (CSIS, Brookings, CFR, RAND and CSIS). A clear majority of the respondents thought that think tanks influence security policy, but this influence is indirect.

Key words: Think Tanks, influence, security policy, United States, policy process

Introduction

There are a number of academics that say think tanks have little or no influence on public policy.[167] Dror rated the performance of think tanks as being rather disappointing in terms of their ability to influence policy. Do the findings of the questionnaires in this research confirm that result? In an era of increasing budget constraints upon governments around the world, which has resulted in diminishing state budgets and cut backs in the state machinery, has exerted effects upon the state's ability and role in policy identification, formulation and implementation. Traditionally, policy has been perceived by some as the domain of states and governments. However, these changes have seen this former monopoly of the state eroded.[168] This situation creates the opportunity for alternative actors to play a greater role in the identification and formulation of policy.[169]

Think tanks are one such actor, which try influence government policy. This article shall focus upon the role of think tanks within the security policy environment in the United States. More specifically the actors are National Security Council, Department of State, Department of Defence, and additionally the

[167] Yehezkel Dror, "Required Breakthroughs in Think Tanks," *Policy Sciences* 16, 1984, pp. 199-225; Richard Higgot & Diane Stone, "The Limits of Foreign Influence: Foreign Policy Think Tanks in Britain and the USA," *Review of International Studies* 20(1), January 1994, pp. 15-34.

[168] R Kent Weaver, "The Changing World of Think Tanks," *P.S.: Political Science and Politics* 22, September 1989, pp. 563-579; Geoff Mulgan, "Thinking in Tanks: The Changing Ecology of Political Ideas," *The Political Quarterly* 77(2), April-June 2006, pp. 147-155, p. 18.

[169] R Kent Weaver, "The Changing World of Think Tanks"; Murray Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks* (New Brunswick (NJ): Transaction Publishers, 2011).

Department of Homeland Security and Department of Justice when it comes to Strategic Counter Terrorism Policy. Under these Cabinet Departments should also be added their relevant agencies. It has been hard to find any overview of think tanks influence in general. John Kingdon had a somewhat larger category of "researchers, academicians and consultants" when he did his study on Non-Governmental Actors influence on US political decision making.[170]

Given the current critical juncture of the above mentioned changes in government and the state of global affairs/relations, understanding who and how security policy is influenced is crucial. Just how they do achieve this has been the cause for some heated debate. This is influenced by how academics and practitioners view the security policy environment in the United States, such as whether it is a closed or an open system. And whether the policy system is open to pluralistic sources of input or is an elitist project.[171]

In a number of regards the US policy environment is rather a special and specific environment. The findings of an article, which appeared in the Journal of Policy Studies in 2010 (Nicander),[172] seemed to indicate a faster degree of change in US Security Policy – from identifying a possible new threat paradigm until legislating and implementing preventive and protecting measures within the society.

There are issues and processes that make the understanding the issue of influence on foreign and security policy even more critical is the extremely volatile nature of international politics within the current frames of the *Global War On Terrorism* and the *Arab Spring*. It is critical to get the right policy to address the right problems. Understanding how policy is influenced is the first modest step in this direction.

This paper forms part of a larger project concerning bureaucratic ability to adapt or change to circumstances in the security policy environment. Other aspects are analysed in different papers, but it is the intention of this article to broach the following problematic question, what influence (direct or indirect) do the relatively independent/bipartisan think tanks have within the security policy domain in the US? This question immediately imposes upon a scholar the necessity of defining *influence* and discusses ways and means of measuring it. This shall be done from the point of view of an academic's theoretical lens as well as from the point of view of a practitioner. By setting about answering the research question in this manner, contradictions between the theoretical (academic) and practical (policy makers/practitioners) shall be exposed. The

[170] John W. Kingdon, *Agendas, Alternatives, and Public Policies*, 2nd Edition, (New York: Pearson, 2011), p. 54.

[171] Donald E. Abelson, *Capitol Idea: Think Tanks and US Foreign Policy* (Montreal: McGill-Queens University Press, 2006); R Kent Weaver, "The Changing World of Think Tanks"; Murray Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks*; Eric Swank, "Clinton's Domestic Policy Makers," *Journal of Poverty* 2(1), 1998, pp. 55-78.

[172] Lars Nicander, "Shielding the Net – Understanding the Issue of Vulnerability and Threat to the Information Society," *Policy Studies* 31(3), 2010, pp. 283-300.

primary intention is to generate an overview and learned discussion on the aspect of assessed or perceived influence. As such, this does not mean that influence needs to take place, but what strategies and tactics academics, policy makers and practitioners believe are successful. Given the size and nature of think tanks in the United States, if there is no influence found in this specific environment, it is less likely to be found elsewhere.

After the theoretical definition and framing on how the term Think Tank is understood in this context, follows a description of what makes the US Think Tank environment special and its unique character in relation to think tanks in other countries. This is followed by a review of the states of theories on the role of think tanks in general and some relevant schools of thought. A questionnaire was distributed to establish the views and experience of established professionals working in the field, in order to understand the practitioners' lens and understanding of the issue. Respondents were chosen on the basis of the length of service in think tanks, government and academia, in order to offer useful insights by experienced people that have served in all of the parts that potentially contribute to the policy process. The outcome of this questionnaire was then compared with the theory findings, how the Think tanks operate and also on their influences in Congress. Information gleaned from the questionnaires was enhanced with a qualitative approach based on in-depth interviews[173] with those who agreed to be contacted further (from the pool of those that had received and responded to the questionnaire) to give a more comprehensive understanding of the 'insider's perspective'.

Theoretical and Analytical Framework

The General Role and Character of Think Tanks

In brief, a Think Tank can be described as an organization that fills the gap between knowledge and decision making. According to a more detailed definition, think tanks are defined as: Think tanks are public policy research, analysis and engagement institutions that generate policy-oriented research, analysis and advice on domestic and international issues that enables policymakers and the public to make informed decisions about public policy issues. Think tanks may be affiliated or independent institutions and are structured as permanent bodies, not ad hoc commissions. These institutions often act as a bridge between the academic and policymaking communities, serving in the public interest as an independent voice that translates applied and basic research into a language and form that is understandable, reliable, and accessible for policymakers and the public.[174]

[173] The 18 respondents – interviewed through personal meetings (F2F), through Skype and by phone - have been renamed to R1 through R18 because of confidentiality issues, quotes from all respondents have not been used to highlight claims in this article but will be forwarded in upcoming articles on the same subject.

[174] James G. McGann & Erik C. Johnson, *Comparative Think Tanks, Politics and Public*

Think tanks can be classified in several different ways.[175] According to one model, they can be classified according to their degree of independence from the state. However, usually think tanks are classified according to their primary mission and focus, usually labelled as either 'university without students', 'contract researchers', and 'advocacy centres'. A fourth category is sometimes used in the United States, so-called 'vanity/legacy centres', a category that is usually associated to a former president and his 'presidential library'.

The first category, 'Universities without students', is considered to be the most independent and usually has more than fifty employees. Often, researchers and scholars who are trying to get away from teaching and administrative duties gravitate towards this type of employment. Other groups that are attracted to this type of work consist of conservative scholars who think that the academic world is too radical and leftist as well as former diplomats and civil servants who lack a traditional academic background (i.e., they do not have a PhD). The typical products ('output') that this type of Think Tank produce are primarily aimed at decision makers, and usually consist of rather detailed monographs of primary research. The Brookings Institution (Washington D.C.), the Centre for Strategic and International Studies (Washington D.C.), Council of Foreign Relations (NYC), and the Hoover Institution (Stanford, CA) are well known examples of this category of think tanks.

The second category 'government contractors' are formally called Federally Funded Research and Development Centres (FFRDCs)[176], and usually operated within in the security and defence sector. These institutions usually has special access and operate 'in-house' with the customer in order to solve a specific problem. This category of think tanks depends upon their size and having a substantial amount of customers in order to maintain their balance and integrity. Both RAND (Santa Monica, CA) and Urban Institute (Washington D.C.) falls in to this category; however, the latter only deals with issues related to welfare and the organization of society on a local and regional level.

There is an additional category of independent think tanks, 'advocacy centres'. This type of Think Tank is usually ideology oriented and advances various policies and policy solutions based upon a certain political philosophy. Often the conservative Heritage Foundation (Washington D.C.) and American Enterprise Institute (Washington D.C.) are labelled as being advocacy centres, but a better example is actually the libertarian Cato Institute (Washington D.C.). The line between 'advocacy oriented' think tanks and what in Scandinavia is referred to as PR and lobbying firms is somewhat more fluid. This is the main

Policy (Northhampton (MA): Edward Elgar Publishing, 2005); James G. McGann, *Think Tanks and Policy Advice in the US: Academics, Advisors and Advocates* (New York: Routledge, 2007).

[175] R Kent Weaver, "The Changing World of Think Tanks."

[176] FFRDCs conduct research for the United States Government. They are administered in accordance with U.S Code of Federal Regulations, Title 48, Part 35, Section 35.017 by universities and corporations. http://www.nsf.gov/statistics/ffrdclist/gennotes.cfm och http://www.nsf.gov/statistics/nsf05306/

reason why this paper is focused on the independent think tanks that primarily work with security policy decision making.

The Think Tank industry was developed in the United States during the second decade of the 20th century, about the time of the Great War (1914-18). Since then, this industry has been through several periods of change. Today there are more than 6000 think tanks in more than ninety countries; the largest concentration – approximately 1700 - is found in the United States.[177] This is a rapidly growing industry. According to Weaver,[178] "think tanks are more numerous and probably play a more influential role in the United States than in most other western democracies." Following from this assumption, if Think Tank influence on policy can be found, it is more likely to be found through a study on Think Tank influence on policy in the United States.

A number of works have been written on the think tanks strong position in the United States compared to Europe; a usual explanation to this phenomenon is that the think tanks in some aspects compensate for the lack of a culture of strong political parties that is common in most European countries[179]. Due to the balance of power between the American president and the Congress - and the fact that American political parties mostly function as election machines – the members of the Congress have a greater need for qualified knowledge and information; in addition to this, they also have more freedom compared to most European members of parliament. Gray[180] states that US think tanks are able to inform and influence policy due to two primary reasons. Firstly, their views are deemed legitimate by officials. Secondly, that staff of think tanks are well qualified and may in fact also be former officials. Today, the leading independent Think Tank in Europe in widely believed to be the German Stiftung für Wissenschaft und Politik (SFW).

Theories on Think Tanks

There are a number of scholars who are most active in the research field of think tanks, such as Donald E. Abelson, James McGann, Diane Stone and Andrew Denham. Abelson has also written a case study on two security policy situations - the ABM/SDI-decision and the global war on terror GWOT – in order to analyse the role of think tanks in these events even though these situations could be analysed in several different ways. Murray Weidenbaum (Competition of Ideas 2011) argues that Abelson's "description of think tank activity is useful,"[181] even though this particular concept cannot explain it completely.

[177] James G. McGann, *2012 Global Go to Think Tanks Report and Policy Advice* (Philadelphia: University of Pennsylvania, 2013), p. 24.

[178] R Kent Weaver, "The Changing World of Think Tanks," p. 570.

[179] See among others Kent Weaver, The changing world of Think-Tanks, page 570 in PS: Political Science & Politics, 1989

[180] Colin S. Gray, "'Think Tanks' and Public Policy," *International Journal* 33(1) Opinion and Policy, Winter 1977/1978, pp. 177-194, p. 190.

[181] Murray Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks*, p. 58.

A number of theoretical attempts have been undertaken to try and capture the nature and essence of organisational influence on the policy process.

According to Abelson there are four separate schools of thought that can be used to analyse and conceptualize think tanks. The ***elitist***[182] school argues that think tanks are an integrated part of the power structure in the United States in the form of knowledge banks and talent pools for future presidential administrations. Unfortunately, these thoughts are often paired with another approach, influenced by Marxism. According to this approach, the role of think tanks is to support and advance its donors direct economic and political interests.[183] It is reasonable and possible to support the former approach without at the same time accepting the latter, as has been emphasized Abelson. This is also the main reason according to Abelson, the reason this school of thought sometimes is perceived as being imprecise, contradictory and has a slight dichotomy to its nature.

The ***pluralistic***[184] argue that think tanks are a part of a strong pluralistic American tradition in which this type of organization only forms a small part of the body that shapes the American decision making; this is made up of unions and a number of different organizations that promote and protect various interests. Ultimately, it is the state that will deliver some form of verdict or decision regarding a certain interest (i.e. in the form of its congress and administration).

The ***statist***[185] school use an approach that is based upon the vision that the state completely and independently formulates political goals that it tries to achieve despite national and international resistance. Decisions and policies on foreign policy are shaped by its most important actors, the President and the Secretary of State. That is, foreign policy and issues on national security are controlled by the White House and the State Department. This approach may imply that think tanks play a rather modest role. However, the importance of the 'the revolving door' with experts who are recruited from think tanks to closed, policy making environments or vice versa, is of great importance. Both the White House and the State Department depend upon advisers and experts;

[182] Joseph G. Peschek, *Policy-Planning Organisations: Elite Agendas and America's Rightward Turn* (Philadelphia: Temple University Press, 1987); Thomas R. Dye, *Who's Running America?*, 4th Edition (Englewood Cliffs (NJ): Prentice-Hall, 1986); G. William Domhoff, "Social Clubs, Policy Planning Groups, and Corporations: A Network Study of Ruling-Class Cohesiveness," *Insurgent Sociologist* 5(3), 1975, pp. 173-184; John S. Saloma (III), *Ominous Politics: The New Conservative Labyrinth* (New York: Hill & Wang, 1984).

[183] G. William Domhoff, "Social Clubs, Policy Planning Groups, and Corporations: A Network Study of Ruling-Class Cohesiveness."

[184] David Newsom, "Foreign Policy and Academia," *Foreign Policy* 101, 1995-1996, pp. 52-67.

[185] Theda Skocpol, Government Activism and the Reorganisation of American Civic Democracy, Paper given at the conference The Transformation of the American Polity, (Cambridge (MA): Harvard University. 3-4 December 2004); Stephen Krasner, Structural Conflict, (Berkeley: University of California Press, 1985).

it is a logical conclusion that think tanks are in a position to influence the decision making process.

The ***institutional***[186] school use an approach that analyses think tanks and their individual researchers as parts of a policy and expertise network, and how they cluster in different decision making situations. The benefit with this approach is that scholars can get a deeper understanding of the 'sub government' by analysing primary sources such as transcripts of meetings, protocols, and other documents that have been used. However, the lack of other sources creates a picture that can have some limitations. This school of thought is also known for its discussion on 'agenda setting'[187] and its focus on the phase in the decision making process where different institutions and interests gather in order to promote their ideas.

In reflection, it can be said that no one single school of thought or theory can explain the role of think tanks in the policy making process; an integrated approach is often necessary unless one is studying a specific situation. As an example it can be said that the static approach might be the most useful in order to explain the decision making process before the invasion of Iraq 2003; in this case a group known as the 'Vulcans' (e.g. Wolfowitz and Cheney) all had links to the same Think Tank (in this case PNAC). This particular group of people formed a very tight and closed group that had strong connections to President George W. Bush. An example of an integrated approach could be to apply Weidenbaum's opinions on Abelson's theoretical arguments.

Weidenbaum (The Competition of Ideas, 2011) partly supports this position and underlines the difficulties to measure with any degree of reliability and validity the influence of think tanks on the policy process. Instead, he promotes the idea of the indirect influence of scholars; they compile and analyse material that otherwise might be difficult to access. A group of particularly important recipients are staffs that work for members of the U.S. Congress, and especially those who work for various Congressional committees.

In addition, Donald Abelson has (2005) made a number of interesting observations regarding the American think tank environment. Two trends stand out. The first observation Abelson made was that "many contemporary institutes have made and continue to make a concerted effort to influence public opinion and public policy. Rather than debating the advantages and disadvantages of various domestic and foreign policies from the comfort of their

[186] Hugh Helco, "Issue Networks and the Executive Establishment," In Anthony King (Ed.), *The New American Political System* (Washington DC: American Enterprise Institute Press, 1978); Evert A. Lindquist, "Think Tanks or Clubs? Assessing the Influence and Roles of Canadian Policy Institutes," *Canadian Public Administration* 36(4), December 1993, pp. 547-579; Diane Stone, *Capturing the Political Imagination: Think Tanks and the Policy Process* (Portland (OR): Frank Cass, 1996).

[187] John W. Kingdon, *Agendas, Alternatives, and Public Policies*; Denis Stairs, "Will and Circumstance and the Postwar Study of Canada's Foreign Policy International Journal," *Canada's Journal of Global Policy Analysis* 50, March 1995, pp. 9-39.

book lined offices, think tanks, particularly those advocacy-oriented, prefer becoming active participants in the political arena" (preface). In other words, there is an attempt to influence the public debate regarding specific issues, and by doing so having an indirect influence on policy.

The other, and perhaps more relevant observation is linked to the role think tanks play by being able to influence the public debate and discourses on policy issues by developing certain strategies in order to be competitive on the 'idea and influence market'. Think tanks have very shifting internal and external resources (e.g. access to media). The historian James Smith has noted that "think tanks have become all too savvy at competing in the market place of ideas".[188] The ability of a Think Tank to promote itself and transfer its ideas in a wider, public context is because of this a key factor for its influence. This idea was expressed by most of the second round interviewees, who noted it is not only about having good ideas, but letting others know you have them. A selection of quotes includes:

- "Traditional publishing [...] new social media, you have to be innovative with Facebook, Twitter, the whole list of things. Blogs potential, I notice a lot of think tanks that are very active, their scholars have blogs. Television, debating on television, media strategy, magazine, periodicals, influential sort of opinion in your field. All those things. You have to use everything these days" (R17[189], 120703, Skype).
- "I think getting time with the senior director at the NAC is extremely hard. I do not think you can assume that is your principle audience unless the idea has already been highlighted with an op-ed or some other media event that would grab the attention of a senior director" (R15[190], 120702, telephone).
- "Media savvy?" "Exactly, that is the way they put it. They get their views out very quickly, whenever there is an event in the world or some new development where their expertise would be sought. So those are some of the reasons." (R17, 120703, Skype).

These quotes demonstrate the way that think tanks try to stand out in a crowded marketplace if ideas. It is about getting your ideas and capabilities out in the public to be noticed, and with luck to gain some traction. Abelson's categorization of think tanks from four theoretical approaches has been analysed by Weidenbaum regarding their relevance and substance. Firstly, *elite organizations* that depend upon experts and close ties to policy makers do so in order to support their sponsors' political and economic interests. Due to the

[188] Donald E. Abelson, *Capitol Idea: Think Tanks and US Foreign Policy*, preface.

[189] R17: Senior counsel and co-author to the 9/11 Commission, former CIA officer, consultant to Homeland Security projects and Bipartisan Policy Center, CT advisor to the State Department and to the Nuclear Threat Initiative, 25 years of experience within the US Security Policy environment and US Government.

[190] R15: Adjunct professor at Georgetown University, former career intelligence analyst at the CIA, former National Intelligence Officer, over 30 years of experience within the US Security Policy environment and US Government.

fact that this school of thought houses two hypotheses that are often wrongfully associated with each other – the talent pool for coming administrations on the one side and the purpose of supporting its sponsors on the other side – makes it rather difficult to analyse which hypothesis a study actually uses. Due to this methodological problem, Weidenbaum rejects this categorization made by Abelson, even though the latter has publicly stated that he does not support the hypothesis that is influenced by Marxism.

The interviewees all separated the two parts of this thesis insofar as that they agree that think tanks are acting as talent pools for administrations. However, reject the notion of partisanship, which they believe ruins a Think Tank's brand and reputation and is therefore counter-productive. Thus the networks are vital as is the idea of objectivity.

- "Somewhat the revolving door, I think on a lower level it tends to be dynamic" (R3[191], 120413, telephone).
- "There are a lot of senior experts, senior fellows that tend to be there [at think tanks] when they are not in government, there are different administrations" (R18[192], 120705, F2F).
- "The most important factor is objectivity and being able to speak truth to power" (R1[193], 120406, telephone).
- "If you are trying to gain trust and credibility, objectivity is a critical piece. But I think that there are so many disincentives to objectivity that it is almost impossible to maintain it" (R4[194], 120416, telephone).

The last quote was interesting insofar as it notes that objectivity is desired, but the environment makes it very difficult to maintain. Secondly, think tanks can be regarded as just one of several actors in a constantly growing and "crowded marketplace of ideas". This position is supported by Weidenbaum. Thirdly, think tanks play a modest role in the shaping of policy compared to the administration's power and resources. Weidenbaum partly supports this approach, adding that this influence can be of a vital and strategic character at certain moments. He does not express any direct opinions that are limited to

[191] R3: Senior Risk Management scientist in the DHS Science and Technology Directorate, former Federal On-Scene Coordinator for several major incidents, 7 years of experience in the central government and 30 years of experience in the Coast Guard.

[192] R18: Served as a soldier, a lawyer, a professor, and a diplomat, and has worked for the White House, the Pentagon, the World Bank, the United Nations, and a large international law firm. Currently a senior fellow and adjunct professor at Georgetown University with a total of 15 years of experience within US Security Policy and US Government.

[193] R1: Former Chairman of the Department of Grand Strategy and Mobilization at NDU, served in the US Air Force including two tours to Vietnam, adjunct professor at Georgetown University and over 40 years of experience from within the US Security Policy environment and US Government.

[194] R4: Cultural anthropologist, who works on defense and national security issues, has held positions at a variety of Think Tanks, including RAND and Institute for Defense Analysis, former Scientific Advisor to the United States Army Human Terrain System with a total of 13 years of experience from within the US Security Policy environment and the US Government.

the White House and State Department within the framework for this school of thought.

The fourth school of thought, according to Abelson, think tanks have different mandates and operate under different circumstances. Weidenbaum argues that this is how think tanks operate in very special circumstances that decides whether or not a Think Tank will be involved in the policy making process. Finally, it has to be emphasized that the scholars who are active within this field of research concur, regarding the difficulties of measuring influence; the main reason for this being the lack of hard data regarding the decision making process itself. Weidenbaum's opinions are well suited to develop Abelson's thoughts on the influence the independent think tanks have regarding security policy.

Other significant scholars –McGann, Stone and Denham come to mind – use other approaches in order to explore and analyse this field rather new and uncharted field of research. McGann has studied a number of key factors (political, economic, and policy related) that affects the possibilities of think tanks to offer independent advice and analyses. He used enquiries with employees within the business as respondents in an early research project. This resulted in a divergent interpretation regarding what role different groups believed think tanks should play. One such role was to predict the need of policy development before these needs became obvious, and started to have their own life, sometimes fuelled by special interests.

McGann started to cooperate with Erik C. Johnson in 2005, and wrote a comparative study that measured thirteen indicators of influence in policy-making in different countries such as: political freedom, the political system, number of years as a democracy, number and size of political parties, the type of civil society, freedom of the press, economic freedom, GNP per capita, the public sectors demand for independent policy analysis, the size of the population, philanthropic culture, the number of public and private universities and their degree of independence, the degree of internationalization and global integration (pp. 1-2). This detailed account show a diversity of possible routes of influence, and the think tanks possibilities to survive and influence the policy making process.

Stone and Denham made another comparative study of think tanks in 2004. They also made the conclusion that the interpretations and opinions regarding the Think Tank's role and influence is diverse; some largely overestimate the influence, while other downplay it, sometimes describing it as being non-existent. Stone and Denham appear to lean towards the latter, that the think tanks have almost no influence on the state's development of policies. They state "it is rare to find uncontested examples of a one-to-one correspondence between a think tank report and a policy subsequently adopted by government. [...] Instead, they (the various authors in the book) develop wider and more nuanced understandings of think tanks' policy influence and social relevance in their roles as agenda-setters that create policy narratives that capture the political and public imagination." (p. 11). The value and usefulness of think tanks can be described and interpreted in a more indirect context rather than in direct, causal effects, according to their research.

Two other scholars have conducted research on this matter and have made similar conclusions. The British scholar Geoff Mulgan noted in an interesting article from 2006 (Thinking in Tanks: The Changing Ecology of Political Ideas) how the changing political ecology influence think tanks. The meaning of his observations – who are made in an European context, primarily the United Kingdom - is that it can be the Think Tank's ability to adapt to new circumstances on the political market that are decisive for success and the exploitation of new possibilities.

Ken Weaver at Brookings wrote in 1989 an article (The Changing World of Think-Tanks) who tried to describe the growing number of think tanks, and especially the relatively new category of 'advocacy tanks', who has emerged by the side of the two older and more established types 'Universities without students' and 'non-profit contractors'. It is especially the Heritage Foundation's aggressive marketing that has captured the interest of Weaver; apparently their reports are marketed as being so short that "the decision makers can read them in a limousine ride from National Airport to Capitol Hill".[195]

Weaver argues that think tanks have different purposes and roles. Firstly, as a source for policy specific strategies and action plans; secondly, as a source of and as a tool for evaluation of policy proposals; thirdly, as a tool for evaluation of government programmes, fourthly, as a personnel provider ('government in exile'); and finally, as experts in general. What is so specific about the American system according to Weaver is that it allows for a specific Think Tank influence due to the balance of power between the Congress and the administration, a relatively weak political party system, and a diverse and available body of administrative elites.

An additional factor that Weaver puts forward is the American culture of philanthropy (and the system for tax reductions) for individuals and corporations who support research; this is considered to be a key factor for the growth of think tanks in the United States. Weaver finally notes that there is no single definition or methodology that can be applied in order to explain what a think tank does, how it operates and is financed; what can be said is that the American Think Tank environment is unique, and that the American experiences of think tanks cannot be transferred without adaption to other countries and contexts.

Higgot and Stone[196] have argued that think tanks have evolved over time, and in doing so, may have lost some of their ability to influence policy. They

[195] R Kent Weaver, "The Changing World of Think Tanks," p. 567.

[196] Richard Higgot & Diane Stone, "The Limits of Foreign Influence: Foreign Policy Think Tanks in Britain and the USA," p. 34.

describe the 'old type' of think tanks as being innovative and visionary, being idealistic and club-like in nature. These think tanks relied on scholarship to inform policy. The 'new' variants are much more activist-like and 'hyper-active' in their nature. As such they are more political and instrumental than the earlier form of think tanks. Barley's[197] research also implies an increasing level of vested interests being involved in influencing think tanks and their output, Wisensale's work[198] produces similar results with think tanks purposing a political as opposed to scholarly approach to their work on influencing policy. Yet the increased number of think tanks does not necessarily translate into influence. There are a greater number of conservative think tanks in the US, which possess a greater deal of resources than their liberal counterparts. But this has not greatly increased their influence in proportion to the increased organisational number and resources.[199]

It is interesting to note that a number of respondents (a minority) that thought that think tank influence were marginal. Although this is not part of what is being addressed in this article, it does need to be mentioned. In terms of effect on security policy decision making, 34 per cent of respondents said there was some and three per cent said that there was none (60 per cent answered yes, definitely). These figures approximately corresponded with the perceived level of trust and credibility of think tanks. 34 per cent said there was a neutral level, five per cent thought that the level of trust and credibility was low or very low. Those who saw think tanks having less influence in the future tied much of this to two primary reasons: 1) the lack of funding (including from private foundations), and 2) owing to the existence of too many think tanks with too much overlap in a crowded field.

Convergence Between the Four

There are six points of convergence regarding the think tank phenomenon that can be distinguished between the four scholars Abelson, Weidenbaum, Weaver and Mulgan (the latter operates in a British context).

1/ The market for ideas has become increasingly crowded. 2/ A stellar reputation is the key to survival and success regarding influence and finances. 3/ There exist no single model for the classification of a think tank; different models and versions exists side by side in a heterogenic policy making environment. 4/Think tanks must be able to attract media and the decision makers in order to survive and operate. This can only be achieved if the think tank has access to excellent personnel and activities of a high standard. 5/Think tanks are a hybrid

[197] Stephen R. Barley, "Building an Institutional Field to Corral a Government: A Case to Set an Agenda for Organisation Studies," *Organisation Studies* 31(6), 2010, pp. 777-805, pp. 791-792.

[198] Steven K. Wisensale, "The Family in the Think Tank," *Family Relations* 40(2), April 1991, pp. 199-207.

[199] Andrew Rich, "US Think Tanks and the Intersection of Ideology, Advocacy and Influence," *NIRA Review*, Winter 2001, pp. 54-59, p. 59.

between the academic and the political world. 6/Think tanks do not usually have the objective to influence specific legislation but rather to call for attention and generate a public debate about general policy options.

A preliminary positioning in a matrix

The think tank's role in the Policy process	**Indirect influence**	**Direct influence**
Closed	*Schools* The static school "Non-profit" consult (e.g. RAND): are rewarded government projects for policy support. They have to be chosen due personal contacts or their ability to market suitable projects.	*Schools* The elite school Advocacy Tanks: have a very specific agenda, aiming at influencing the policy process in order to support their own agenda and a specific issue. Their influence is based upon party politics and their connections to the ruling elites.
	Scholars Abelson: Think tanks are elitist organisations but are responsive to the demands of the market (this is also linked to the argument of "modest" influence).	*Scholars*
Open	*Schools* The pluralistic school Universities without students: open competition among think tanks in their struggle for attention and influence.	*Schools* The institutional school
	Scholars Weidenbaum: Think tanks need to compete with each other in order to get attention and influence. However, they have to be careful and not get too deeply involved in the decision process; such an involvement could jeopardize their status as non-profit, which governs taxation.	*Scholars* Mulgan: an open process based upon competition. The think tanks need to be involved in politics, ideologies, and practical policy implementation. The think tanks aim at breaking the public sector's monopoly on policy support. Weaver: The American political process gives think tanks influence, at the same time the public sector's monopoly on policy support has been gone for a long time.

An open system refers to one that is receptive to outsider or external input. A closed system is not open to input from anyone that is not part of the in-group.

In practice, the different theoretical approaches have a tendency to overlap, and the line between the different schools of thought is perhaps not as distinct as the matrix indicates. For example, the pluralistic school does not hinder that the power groups in in the static school also can be observed within the framework of the pluralistic school.

Understanding Influence

To begin with, some framing of the term 'influence' is needed. Robert A. Dahl defines it as "a relation among human actors such that the wants, desires, preferences, or intentions of one or more actors affect the actions, or predispositions to act, of one or more actors in a direction consistent with – and not contrary to – the wants, preferences, or intentions of the influence-wielder(s)".[200] He then narrows down the different ways of understanding influence, where the notions of distribution, gradation, scope and domain can serve as guides to the observation and analysis of influence.

Yet the problem is that a precise and reliable measurement of different actors' influence – especially weighing the scope and domain - does remain difficult in theory as well as in practice, however the centrality of influence seems clear to all political observers. The questions posed by Dahl relating to this study are highly relevant: What persons or groups have the greatest effect on a legislature tax measures? Who tends to initiate proposals, to win others over to them, to carry them through over opposition, to defeat or sidetrack proposals over others? Why do some policy questions never become public issues?

Dahl also refers to Jack Nagel's discussion on causality here. The latter states that direct influence means influence in a specific decision-making process – either in choosing some alternatives or rejecting one or more alternatives. Indirect influence is here more connected with how often think tanks are consulted or constitutes a part of the decision makers' reference framing. Influence is often understood as a "causal connection between an actor's preference on an outcome and maybe also the form of the outcome".[201] Influence is tied to the ability of an individual or organization to persuade its target audience.

The basis of persuasion is not based on 'forcing' a viewpoint or course of action upon another. But it is to present information in such a manner as to convince them to freely choose a particular point of view or action. Important within this context is that persuasion is influenced by moral components – choosing to engage in morally beneficent actions and choosing to refrain from morally reprehensible ones, for example.[202] This implies the weighing of moral judgements based upon symbolism and values.[203] Perloff defines persuasion as "a symbolic process in which communicators try to convince other people to

[200] Robert Allan Dahl & Bruce Stinebrickner, *Modern Political Analysis*, 6th Edition (Upper Saddle River (NJ): Pearson Publishing, 2003), p. 17.

[201] John H. Nagel, *The Descriptive Analysis of Power* (New Haven (Connecticut): Yale University Press, 1975), pp. 29 & 55.

[202] Richard M. Perloff, *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*, 4th Edition (New York: Routledge, 2010), p. 11.

[203] Richard M. Perloff, *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*, p. 12.

change their attitudes and behaviours regarding an issue through the transmission of a message in an atmosphere of free choice."[204]

Persuasion involves five different components to it. 1) It is a symbolic process, 2) involves an attempt to influence, 3) people persuade themselves, 4) involves the transmission of a message and 5) requires free choice.[205] In terms of impact, persuasion can be used for three broad effects. One effect is to **shape** attitudes and opinions on something. A second use is to **reinforce** attitudes and opinions in an audience. The third effect is to **change** attitudes and opinions.[206] This now needs to be tied back to think tanks and how they embark upon attempting to persuade (and influence) policy makers.

Weidenbaum (2011) studied the influence of think tanks in Washington DC from a more general perspective. He finds that this influence is generally underestimated and he is somewhat critical of the present schools of research in this area. Interviewees (in the second round) seemed to be split about the influence of think tanks on the policy process. The different camps agreed that influence did in fact occur, but for quite different reasons. One camp spoke of broadening the dialogue and debate on an issue or policy, and another that think tanks were used as a kind of 'rubber stamp' for a pre-determined policy.

- "I think think tanks influence policy by presenting new ideas so that they help to further the debate. They also help influence policy by actually doing the work the government officials very often do not have the time to do themselves, they are busy working on so many issues, that think tanks help to bring a knowledge that would otherwise not exist in government" (R9[207], 120517, Skype).

- "They can be tremendously influential but sometimes only because the conclusions or the think tanks are the way of validating the policy" (R13[208], 120615, Skype).

There are at least three problems that make measuring of influence problematic: Different channels for influence, the existence of counteractive lobbying and the fact that influence can conducted at different stages of the policy process.[209] Thomas Medvetz - an institutionalist – argues that maybe the most

[204] Ibid.

[205] Richard M. Perloff, *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*, pp. 12-15.

[206] Richard M. Perloff, *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*, pp. 24-25.

[207] R9: Founder and Director of Center on Global Counterterrorism Cooperation, lecturer in CT and US foreign policy, Senior Fellow at John Hopkins University, and nonresident Senior Fellow at George Washington University, a total of 14 years of experience from within the US Security Policy environment.

[208] R13: 37 years of government service including Assistant Inspector General for Security Oversight, Senior Advisor for Policy to the assistant Secretary of Defense, Assistant Secretary of State, and Director for Intelligence Policy.

[209] Andreas Dür, "Measuring Interest Group Influence in the EU: A Note on Methodology," Forum Section *European Union Politics* 9(4), 2008, pp. 559-576, p. 561.

important effect of Think Tank influence is not to promote own proposals, but to ensure that inferior alternatives are weeded out, which makes it even harder to state causality.[210] Sun Zhiru and Zhang Zhiqiang[211] propose that a quantitative text analysis can be undertaken to measure influence. This is done by comparing a Think Tank's policy position with the final policy output. Their argument is that this allows for assessing the preference realisation of think tanks in the decision-making process.

Think Tanks must compete with one another in an increasingly crowded marketplace of ideas, which demands innovative strategies in order to attract the attention of policy makers. The main methodological element of this research approach was a two tier questionnaire to respondents with an 'insider's perspective' on the US think tank environment to possible derive their role and influence. In this article the focus is on the outcome of the quantitative part and also an overview on think tank influence in Congress. The research question is thus narrowed down to "What think tanks are most influential in the US security policy domain", which is based on the assumption that they do exercise significant influence.

Empirics and Analysis of the Influence of Think Tanks - Two Approaches

Questionnaire With an Insider Perspective (Quantitative)

An important basic assumption for this questionnaire for both active and retired public officials was to find out whether or not think tanks were perceived as having any influence on security policy, and who the most successful think tank are. The result was later on used in order to identify common denominators.

The questionnaire was emailed to approximately 270 respondents in the United States; thirty-five of them answered. One major reason for the lack of response was that the DoD, the State Department and the such have very powerful firewalls that does not allow emails from overseas that could be characterized as bulk e-mails. Several of the respondents were 'friends of friends', who do not know me personally and due to this could not verify me as the sender. I also tried to use a digital signature on my e-mails in order to prove my 'bona fide credentials'; however, that created even more problems with the firewalls. An additional second round, of in-depth interviews with 18 of the original 35 (that agreed to be contacted further) took place via Skype and via telephone. The questions in the second round were designed to tease out answers raised by the initial questionnaire.

[210] Thomas Medvetz, *Think Tanks in America* (Chicago: The University of Chicago Press, 2012).

[211] Sun Zhiru & Zhang Zhiqiang, *Measuring Think Tank Influence Using Quantitative Text Analysis* (International Conference on Information, Business and Education Technology: Atlantis Press, 2013).

The 35 senior respondents were highly qualified. On average, they had served for twenty-two years within the administration, working with security policy; due to their experience they had the right background as customers to think tanks. 18 of the respondents accepted to do a qualitative interview during the second phase of my project.

The most striking finding was that 94 per cent of the respondents thought that think tanks have influence and an impact on decisions regarding security policy in the United States. 60 per cent of the respondents believed that think tanks are held in high esteem regarding security policy. 77 per cent thought that think tank work as a 'talent pool' for coming presidential administrations. The result was somewhat equivocal regarding the argument that think tanks are a part of the policy generating environment in which the best ideas becomes successful on an open and free market, which implies that other factors such as networks, media policy and so forth, plays an important role. Due to this, it is logical that 80 per cent of the respondents believe that the primary strategy for success for think tanks are based upon networking; 77 per cent of the respondents think it is important for the think tanks to carefully consider at which phase they should start to find a place in the policy process.

The study showed that the most important level for influencing the decision makers are the congressional staffers on Capitol Hill and the so-called GS-15 (directors within departments and agencies) – not the politically appointed Under Secretaries and Assistant Secretaries. In other words, the highest political level – ministers, senators and members of Congress – appears to be rather uninteresting as recipients of the work and efforts of think tanks. An answer as to a possible avenue for influence at the level of Congressional staffers and GS 15-level officials is found in some recurring answers given by the respondents. Of particular interest is that these staffers may integrate think tanks findings into governmental analysis. Therefore this may affect the perceived level of trust and credibility by senior policy makers in the material, owing to the source (seemingly governmental as opposed to think tanks). The importance of establishing personal networks in order to influence decision-making was also highlighted as being of critical importance for think tanks in a study by Rich and Weaver.[212]

The five most important 'bipartisan' think tanks that work with security policies are according to the respondents the Centre for Strategic and International Studies (CSIS), Brookings, Council of Foreign Relations (CFR), RAND, and the new Centre for New American Security (CNAS). Therefore, the importance of other significant actors such as the Heritage Foundation are downplayed, mostly due to the fact that they have a tendency to develop towards becoming an 'advocacy centre', with a considerably conservative bias rather than as independent experts. All of these think tanks are primarily active within "The

[212] Andrew Rich & R. Kent Weaver, "Think Tanks in the US Media," *The Harvard International Journal of Press/Politics* 5(4), 2000, pp. 81-103.

Beltway" in Washington D.C., with the exception of CFR, which is based in New York.

Another finding of interest is that 77 per cent of the respondents anticipate that the influence of the think tanks will remain unchanged. Such a result would indicate a very stable system that is also rather closed due to already existing structures, which makes it difficult for new actors to gain access to the system. CNAS is only six years old and rather modest for its size, but might be an exception; it appears as CNAS is able to compensate its small staff with a few highly qualified key people and relevant networks.

Think tanks influence in the U.S. Congress

When the respondents in the first round of interviews rated the think tanks that work with security related issues, five think tanks emerged as being especially noteworthy, also known as 'The big five' (CSIS, Brookings, CFR, RAND, and CNAS). In order to verify these ratings, an analysis was done in order to find out how often these actors could be noticed in relevant congressional hearings and sub-committees (budget, foreign policy, defence and justice) during the period 2007-2012.

This analysis showed that in the House of Representatives, 'the big five' were involved in some capacity on ninety-three occasions; fifteen other think tanks were involved on eighty-eight occasions. This is even more obvious in the Senate – who is supposedly less polarized, and operates with a longer time frame – 'the big five' were involved on fifty-eight occasions; the other fifteen were involved on twenty-one occasions. Usually, three outside experts are called to a congressional hearing in order to highlight the issue. Two of these are nominated by the majority and minority side; the third person is usually an independent expert, and it is here that think tanks play a role by providing fact based recommendations.

It is the responsibility of the individual members of Congress and the staff on the committees to inform themselves regarding different issues, especially issues regarding security policy that might be difficult to gain access to. The main reason for this is that the American political system lacks a parliamentary political system as opposed to the rest of the Western World. There are still voices such as Michael Rich (the director of RAND) who are concerned that the members of Congress becomes increasingly polarized, and rather uses their conviction than empirical facts; if facts happen to support one side, the other side feel a need almost by default to be against it.

The verification of the influence of 'the big five' became interesting and useful discovery process in preparation for the following qualitative interviews, and especially to investigate what characterizes them.

Analysis of the Discrepancies Between the Answers from Scholars and Practitioners

It can initially be noted that the framework provided by the previously mentioned scholars (McCann, Weaver, Stone, Denham, and Johnson) were not so useful for the focus of this study. Denham and Stone rejects completely any form of influence in the government's policy development; a position that turned out to wrong in this context. The indirect influence they advocate must be interpreted as being done by public opinion and media in this case.

Abelson on the other hand, appears to be correct regarding the important role that think tanks play, even though this role might be difficult to conceptualize. The answers indicate that it is to some degree by a combination of the elitist and institutional schools that describes the role of the think tanks best. The elitist school is, however, too complex as a model, since it is possible to accept the thought that think tanks form a talent pool for coming administrations while at the same time rejecting the thoughts that are inspired by Marxism, i.e. think tanks primarily exists to support the interests of its donors (e.g. Domhoff). Abelson rejects the latter position, but admit that the theoretical concept of four schools is not complete; his description of them is actually limiting, which has been pointed out by Weidenbaum.

A significant discrepancy compared to Abelson's findings is that 77 per cent of the respondents think that the White House and the State Department are not the two most important actors regarding security policies. This could indicate that this role is either played by other institutions and power centres on a high level that has acquired an increasingly independent role, e.g. DoD and the CIA. It could also indicate that the decisions are done on a lower bureaucratic level (e.g. by the existence of so-called gatekeepers). This could explain why think tanks rely so much on networking with these gatekeepers.

An alternative and perhaps more realistic explanation could be that think tanks exercises influence on security policies and decision making; however, this depends more on their networks than the value of producing policy relevant analysis. This explanation confirms Weidenbaum's conclusions.

Conclusion

The assumed role and influence of think tanks in the United States in general – and on the field of security policy in particular – is unique. This source of competence and expertise appears to fill a stabilizing function and lubricates the ties between politics and administration, which is important since the United States lacks traditional political parties unlike other Western countries. There is also a rather unusual tradition in the United States where the financiers of most think tanks traditionally avoid influencing their work, opinions, and marketing.

This phenomenon has been analysed by using some of the more well-known theories and approaches on this field of research. The result of this has been applied on a questionnaire given to respondents who have been working within the American administration with security related issues for a considerable time. The role of think tanks in a security context has been limited to an American context in my study. From the questionnaires, the findings and indications are:

1. Think tanks have (assumed) influence over the decision making process regarding U.S. security policy (94 per cent).
2. The most important think tanks are thought to be CSIS, Brookings, CFR, RAND, and CNAS. Indirect influence such as networks, appearance in Congress, and other methods that are difficult to measure must be taken into account. The overrepresentation of 'the big five' in a congressional context is worth noting.

The common denominator for four of 'the big five' is that they are perceived as being bi-/non-partisan, politically mainstream, have a solid financial basis, have recruited highly respected employees (scholars, secretaries of state, diplomats), and have been operating for at least forty years. CNAS is an exception; it is considerably smaller, and was created as late as 2004. Despite this, CNAS became highly influential – for example within the Obama-administration - and is considered to be independent even though former employees in some cases have been perceived as being on the right side of the political spectrum (e.g. David Petraeus).

There are four conditions that are necessary to emphasize if one should try to summarize the very specific American environment for think tanks. First of all, the American political system does not have the traditional political parties. This leads to a need for knowledge that is relevant for policy in a long term perspective. Second, the existence of a political 'spoil-system' makes it possible to change civil servants every fourth year: this means that approximately 1000 politically appointed civil servants may have to leave their position every fourth year, which generates a need to re-create institutional knowledge, often by using think tanks. In addition to this, the employees that have to leave their positions are available for recruitment. Third, the American system is known for its philanthropy and generous taxation benefits.

A fourth factor that does not appear in my work but still deserves to be mentioned is the question of access and information availability on equal terms. The United States has a rather young intelligence community, with a culture of "academic outreach" and the secrecy legislation that goes along with this.[213] A consequence of this is that the employees of think tanks have the same access to information as civil servants in the projects they are working on. Due to this, it is not possible to sort out their recommendations just by labelling them as 'uninformed', as sometimes happens in Europe.

The assumption on the role of think tanks in the creation of security policies is that they do play a very important role, and enjoy a great level of trust and confidence within the American bureaucracy. It can also be said that it is not

[213] Lars Nicander, "Understanding Intelligence Community Innovation in the Post-9/11 World." *International Journal of Intelligence and Counterintelligence* 24(3), 2011, pp. 534-568.

enough to just present the best proposals and ideas; their influence is depending on their networking skills. In addition to this comes the indirect influence think tanks can have by being a base for a 'government in exile'. Another factor for success that can be identified is where in the policy process a certain Think Tank choses to focus on.

Another interesting observation is that the most important recipients and consumers of Think Tank products are the people just below the politically appointed level, the 'machinists' so to speak in the political system. This group of people must be able to quickly deliver accurate information to their superiors.

The need and demand for the services of think tanks are believed to remain at the same level for the foreseeable future; this also applies to the structure of independent think tanks that has been studied within the framework of this study (CSIS, Brookings, CFR and RAND). The reason for this is primarily that it takes considerable time to create a trusted brand. In this context, it is worth noting that the newcomer CNAS became the fifth member of this club in only six years.

This review leads to the conclusion that Weidenbaums's 'overlap' on Abelson's theoretical approach regarding the pluralistic school appears to be the most developed theory for an analysis of the think tank phenomenon. Weidenbaum's studies in other fields of research support this argument. Other theories are of a lesser interest based upon the empirical findings in this study. How this influence is being created and evaluated would make an excellent topic for further research.

Two hypotheses – based upon the pluralistic school – appear to be of importance for a more penetrating analysis against the background of what has been discussed above. First, an important factor for success is independence and integrity. Second, think tanks create their influence and impact to a high degree by using indirect methods such as networks and networks contacts.

Article 5.2

The Recipe For Think Tank Success: From the Insiders' Perspective

Submitted and tentatively accepted for publishing (fall 2015) in
International Journal of Intelligence and Counter Intelligence
by Routledge

Routledge
Taylor & Francis Group

International Journal of Intelligence and CounterIntelligence

ISSN: 0885-0607 (Print) 1521-0561 (Online) Journal homepage: http://www.tandfonline.com/loi/ujic20

The Recipe for Think Tank Success: The Perspective of Insiders

Lars Nicander

To cite this article: Lars Nicander (2016) The Recipe for Think Tank Success: The Perspective of Insiders, International Journal of Intelligence and CounterIntelligence, 29:4, 738-759, DOI: 10.1080/08850607.2016.1177397

To link to this article: http://dx.doi.org/10.1080/08850607.2016.1177397

Published online: 13 Jun 2016.

International Journal of Intelligence and CounterIntelligence, 29: 738–759, 2016
Copyright © Taylor & Francis Group, LLC
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2016.1177397

LARS NICANDER

The Recipe for Think Tank Success: The Perspective of Insiders

Think tanks have, over time, been able to gain considerable success in influencing the security policy process in the United States. Success can be understood as the ability to influence the policy process at some stage and in some manner—anywhere from identifying a "problem" or opportunity to implementing policy. The role of U.S. think tanks, in theory and practice, and whether think tanks had a significant influence in the U.S. national security domain, was previously discussed in these pages.[1] The outcome was a clear "yes," and the five highest ranking think tanks were highlighted.

The focus here is on the why and how on the issue of influencing policy. Several experienced experts in the field had their viewpoints recorded through a series of questionnaires and interviews. A number of strategies and tactics became apparent—revolving doors and networks, publishing and marketing, niching and branding, reputation and profile. The extensive material collected from the experts provides a useful insider perspective that contributes to developing the understanding of how think tanks gain influence in policy.

Increasing budget constraints and demands for tax decreases have resulted in reductions to state budgets and forced the making of cuts in the state

Lars Nicander is Director of the Centre for Asymmetric Threat Studies at the Swedish National Defence College, Stockholm. From 1997 to 2002, he was Secretary of the Cabinet Working-Group on Defensive Information Operations. A political scientist, Mr. Nicander has served in various positions within the Swedish national security environment. He is an elected member of the Institute of Strategic Studies in London and a Fellow of The Royal Swedish Academy of War Sciences.

machinery of numerous governments around the globe. Scholars like Geoff Mulgan thus imply that the perceived traditional government monopoly on policy advice has been broken.[2] In turn, the ability to identify, frame, and implement policies has been affected. This tendency has thereby created opportunities for non-state actors to position themselves in questions of policy identification and formulation.[3]

Think tanks fall into the category of non-state actors trying to affect governmental policy development. Even though the concept of think tanks originated in Europe, with the Royal United Services Institute (RUSI) as the oldest, dating from 1831, United States think tanks now occupy by far the most prominent place when influencing political decisionmaking, particularly in areas related to security policy. Also, they tend to be concentrated in Washington, DC, where the majority of the world's think tanks are located,[4] as are those most heavily funded.

Given these current critical changes, understanding how security policy is influenced is crucial. The ways in which think tanks set out to influence policy are diverse.[5] The manner in which this influence emerges and is interpreted has been subject to intensive debate among scholars, centering on whether the system is closed[6] or open,[7] and whether the policy process is open to plural sources[8] of input in contrast to elitist projects.[9]

The focus here is on the role of think tanks within the federal security policy environment of the United States, more specifically, on the National Security Council (NSC), Department of State (DoS), Department of Defense (DoD), and the Director of National Intelligence (DNI). Also involved are the Department of Homeland Security (DHS) and the Department of Justice (DoJ), in regard to domestic security and counterterrorism. Additionally, other relevant agencies[10] are included, as are the congressional committees linked to these areas.

The results cited here, coming from a follow-up series of interviews to questionnaires that were previously distributed to a group of highly experienced individuals working within the U.S. security and foreign policy environments, provide unique insider perspectives. They also suggest strategies and trends that could become theoretically relevant if and when integrated into the wider academic discussion and debate on think tank influence.

THINK TANKS AND THEIR IMPORTANCE

Considerable debate takes place on the nature of think tanks and how they should operate. From a theoretical perspective, think tanks are viewed in different ways. John Hamre, President of CSIS, noted four different categories of think tanks: (1) architects; (2) general contractors; (3) suppliers; and (4) artisans.[11] Kent Weaver, however, notes only three broad categories of think tanks: (a) historically: universities without students and non-profit government research contractors; and (b) a ‘‘new’’ third model, advocacy tanks.[12] These last organizations combine strong policy, partisan or ideological bias with aggressive salesmanship in order to influence current policy debates. Effective ‘‘spin’’ on existing ideas, and their accessibility to policymakers drives their success.[13]

Think tanks are certainly diverse; Murray Weidenbaum noted five different aspects:

1. Think tank personnel function as both academics and activists at the crossroads of politics and academia;
2. Major think tanks are neither completely conservative nor completely liberal;
3. Differentiation between think tanks and universities is substantial, based mainly on the education of students versus the influencing of public policy;
4. Competition among think tanks is pervasive; and
5. Think tanks make a special contribution to public policy and provide a policy forum featuring knowledgeable and experienced people.

According to Geoff Mulgan, to succeed, think tanks need a subtle understanding of several domains—politics, ideas, and practical policy implementation.[14] Power is derived from being able to straddle these domains. Think tanks, in some regards, can be considered a hybrid of the political and academic environments.

Think tanks can perform a number of different roles. According to Kent Weaver, they are (1) a source of policy ideas; (2) a source and evaluator of policy proposals; (3) evaluators of government programs; (4) a source of personnel; and (5) outlets for punditry.[15] In order to survive in a particularly competitive environment, think tanks need three essential elements: (1) some form of demand for their knowledge and services, especially from political circles; (2) the ability to secure funding from sympathetic donors in order to employ people and run programs and activities; and (3) talented individuals to do the thinking, some of whom may be en route to a political or academic career. This means that they are able to convert political access in to money, money into ideas, and ideas into legitimacy (and attract ambitious contributors by doing so).[16]

At times a lack of clarity can develop between think tanks and lobbying organizations. Gateway House, the Indian Council on Global Relations, has stated that the difference between the two is found in the think tank’s mandate: ‘‘Unlike that of a think tank, a lobbying organisation’s mandate is to influence a policy outcome for a particular interest group. A think tank’s mandate is merely to create innovative policies and hope to influence the policy outcome.’’[17] Another view was expressed by the National Centre for Policy Analysis: ‘‘In recent years, there has been a proliferation of groups who openly advocate public policy changes (usually on a single issue). These groups, however, are not incubators of news ideas. They are better thought of as lobbyists for ideas.''[18] Think tanks and lobby groups may differ in their ability to create new ideas for policy challenges, rather than merely advocating certain ideas and policies on behalf of interested parties.

Another significant difference between think tanks and lobby groups in the United States arises in the legal framework that regulates them. Think tanks are deemed non-partisan, non-profit, research and educational organizations. The Internal Revenue Service (IRS) therefore categorizes them as 501(c)(3) tax exempt organizations. To gain this status, the IRS requires an organization to refrain from attempting to influence legislation as a substantial part of its activities adding that ''it may not participate in any campaign activity for or against political candidates.''[19] While this does not mean that think tanks do not attempt to influence policy, it does mean that doing so needs to be done indirectly.

But things are changing, and the seemingly clear-cut legal and functional lines between think tanks and lobby groups can sometimes become rather blurred. In 2014, the *New York Times* reported on the attempts of various foreign countries (including Qatar, Norway, and the United Arab Emirates) to buy influence via think tanks.[20] A concern, expressed by a lawyer expert on the Foreign Agents' Registration Act (FARA), the statute that governs Americans lobbying for foreign governments, was that ''think tanks have this patina of academic neutrality and objectivity, and that is being compromised.'' This concern demonstrates the value and role played by a think tank's brand and trust in influencing policymakers.

In several regards, the U.S. policy environment is somewhat unique compared to other Western countries. Earlier findings indicated a higher propensity to change—from identifying possible new threat paradigms to legislation, as well as implementing preventive and protecting measures within society—in U.S. security policy compared to other countries.[21] Kent Weaver has explained the U.S. situation as being determined by domestic structural and political factors related to the division of powers between the President and Congress, weak and relatively non-ideological political parties, and the permeability of administrative elites.[22]

The unique role of think tanks as a means to both influence and hasten the degree of change is a timely and relevant area of study. Explaining why and how think tanks have become successful in terms making an impact upon the U.S. policy process provides additional insights to the existing literature on American security policy decisionmaking.[23]

In his study of non-governmental actors that influence on U.S. political decisionmaking, John Kingdon[24] included a somewhat larger category of participants, among them ''researchers, academics and consultants.''

KEY CONCEPTS

Integrity

Independence and integrity appeared to be central issues in the initial distributed questionnaire as explanations for why a think tank scored high in the rankings given by the respondents. This implies that the conclusions arrived at by the producers of reports should be independent with regard to a think tank's management, board, and funders, and that the reports and recommendations should be formulated without consideration of the current political situation.

The five highest ranked think tanks are all found to be independent or "bipartisan": the Center for Strategic International Studies (CSIS), the Brookings Institution, the Council on Foreign Relations (CFR), RAND Corporation, and the Center for a New American Security (CNAS), wherein Democrats and Republicans can professionally work with the same frame of ideas. Other think tanks, featuring a more outspoken policy agenda (e.g., the Heritage Foundation, the American Enterprise Institute, the Cato Institute), are considered to be "advocacy centers" that focus on influencing discussions at a later stage of argumentation, rather than at the earlier stage of policymaking, and seek to generate alternatives.

In this study, RAND has a special status as an independent consultancy, partly inside the American defense system's operational analysis structure, while nonetheless succeeding in keeping to its credo of "speaking truth to power."[25] Doing so is possible, in particular because RAND is not dependent on only one customer, having instead hundreds of opportunities within the U.S. Department of Defense's (DoD) domain. Half of RAND's revenues derive from sources outside the defense community, primarily those within the health sector. This means that RAND is able to balance its customer base, not having to become dependent on a single customer. RAND can thereby stand strong against customers who consider the conclusions in a commissioned report to be unacceptable or unpleasant, and is generally judged impartially as an independent stand-alone think tank.

Network

The joint perception seems to be that the essential way for a think tank to achieve influence is through the use of indirect methods rather than such tangible products as reports and various publicity materials. Several different pathways can be taken to reach influence, but the "revolving door" seems to have a special status. Primarily, this refers to the usual flow of politically-appointed civil servants in U.S. administrations, especially during shifts in the presidency when approximately 1,000 officials may have to leave their positions (the "spoils system"). Many of these individuals end up at think tanks, depending on their insight and knowledge. Politically expert staff members tend to follow them to these institutions.

In reverse, think tank personnel who have been working long-term on a certain issue become attractive for a sympathetic new administration. When in office they tend to turn to their former workplaces for advice or to commission reports. No formal connections exist between those working at a think tank and a government department, but, think tanks constitute both pools of talent and places to store talented researchers and experts. This example of John Hamre was offered by one of the respondents in the interview round:

> I will give you a non-classified example. John Hamre was asked to go to Iraq and take a look at what was going on. And he wrote a report back. Now, if he was not President of CSIS, he might still have been asked since he had been a former deputy secretary of defense. But he was the President of CSIS; it was kind of a CSIS effort, because he had the CSIS supporting him, but CSIS in that case almost became an adjunct of the government. (R6, 09-05-2012, F2F)

Another approach, like the CFR's, is to have a ‘‘Fellow system,'' with approximately 1,000 members and recurring seminars organized for this selected elite, many of whom have held important positions within various administrations. When in government, the former Fellows tend to take the CFR analyses and assessments into consideration, as well as commission CFR with important studies.[26]

METHODOLOGY

Method and the Respondents

As a follow-up to a previously completed set of quantitative interviews, a round of qualitative interviews was conducted during the spring and summer of 2012. In this round of interviews, eighteen experienced respondents participated, all of whom had been involved with think tanks on several different occasions and in different capacities: ten had been employed by think tanks; eleven had been customers of think tanks; eleven had interacted with think tanks in different projects; and four had been temporary researchers, interns, or the equivalent. On average, the respondents had spent 28 years in the U.S. security policy environment.

The set of individuals judged as most interesting to measure policy influence seemed to be the eleven respondents who had engaged with think tanks as customers, but the views of the other seven from the group of eighteen were also taken into consideration. This set of eleven respondents possessed an average of 32 years' experience in the sector, and their background spanned from a former deputy undersecretary of defense for operational planning to individuals responsible for threat assessments at the National Intelligence Council (NIC) and advisors on the National Security Council (NSC) within the White House.

The total number of respondents, particularly in the first round of the study, which saw a mere 35 out of 350 sent out questionnaires answered, implied that the reply results had to be further refined. The low response rates were due to computer firewalls and other electronic safeguards that prevented the intended recipients from receiving the questionnaire. This necessitated a change in strategy from an originally-intended large scale response to one that identified the important and relevant questions and topics to be broached in the first round, to be followed up in a second round with a more focused set of questions to willing participants from the original respondents. Of the initial 35 respondents, eighteen participated in the qualitative interview, a number deemed positive. Because these eighteen[27] respondents held unique insights into the system, the qualitative aspect can be assumed to outweigh the relatively limited number of participants.

SUMMARY OF FINDINGS IN THE FIRST ROUND (QUESTIONNAIRE)

The main method of approach in the first study was a two-tier questionnaire sent to respondents with an ''insider's perspective'' on the U.S. think tank environment seeking to clarify think tanks' role and, above all, their influence on policy. Direct influence is understood as impact on a specific decisionmaking process, either in choosing or rejecting one or more alternatives, while indirect influence is understood as referring to how often each respective think tank is consulted or constitutes a part of a decisionmaker's frame of reference. According to Jack Nagel, influence is often understood as a ''causal connection between an actor's preference on an outcome and maybe also the form of the outcome.''[28]

The questionnaire's first part posed a quantitative round of questions, as well as conducting a general survey of the influence on target audiences derived from the central research question: *Do think tanks have a possibility to influence the security-related decisionmaking process?*

In the second part of the questionnaire, the research question was limited to: *Which think tanks are most influential in the U.S. security policy domain?* This limitation presupposed that at least some think tanks were assumed to exercise significant influence over the policy process. The high acknowledgment rate in the first survey's key question pertaining to whether think tanks had any significant importance on U.S. security policy planning and decisionmaking was opened up in the second survey, asking how the think tanks had achieved this significance. Exploring this angle further would be done through a series of interviews.

One scholar stands out, offering the closest theoretical explanation to the patterns emerging from analysis of the first questionnaire. Murray Weidenbaum found that this external influence is generally underestimated, and raised some criticism against existing schools of research in the area. In using the pluralistic school as a basis, he offered five conclusions regarding how think tanks function in dealing with various issues:

1. Think tanks are both academics and "activists," standing between the research community and politics.
2. The larger think tanks are neither purely conservative nor liberal.
3. The difference between universities and think tanks is fundamental through the focus on educating students versus influence in political and policy formation.
4. The competition among different think tanks is palpable.
5. Think tanks constitute a particularly important contribution to political and policy development (in the U.S.) through offering a policy forum with competent and qualified expertise.

He also tackled issues of organizational structure and work production processes as additional reasons for the ability of think tanks to project influence on the policy process, with influence often varying according to policy domains. Three significant reasons for think tank influence are:

1. Think tanks can gather groups of experts faster than can universities and civil services to focus on relevant and time critical action and response, e.g., crisis management.
2. Think tanks can penetrate policy processes faster than academic organizations through constant presence and networks in the policy environment. Private publishing opportunities shorten the time span between preparation and publication of new knowledge.
3. Think tanks can accelerate the review processes regarding the research they sponsor through less bureaucratic procedures than at universities and in government. An in-depth interview can shed light on other more important specific aspects. This can include the think tank's base of knowledge and expertise, acting as its "niche" in the decisionmaking process, as well as its knowledge in certain geographic areas.[29]

Think tanks currently possess numerous advantages over other types of organizations that work within the sphere of knowledge production: "Institutionally speaking, the think tank stands between the university and government."[30]

But academia has been criticized for failing to bridge the theory-policy gap: "One of the primary obstacles to building this bridge is the lack of systemic data about when and how academic social science is useful to policymakers."[31] The issues of policy relevance, academic "ivory towers," and their relatively slow speed has put academic institutions at a disadvantage when compared to think tanks.

SECOND ROUND INTERVIEWS: THE WHY AND HOW

Purpose and Approach of the Study

The first round of questionnaires ended with two specific elements identified—integrity and network—being defined as key concepts for a think tank to become successful. Studying why and how came next through interviews featuring an ''insider's perspective.'' Among the variables considered in the study were:

- The unique non-parliamentary system in the U.S. that both permits and requires alternative hubs of knowledge outside the, in this case, relatively weak and streamlined administrative apparatus.
- The political ''spoils system'' in the administration which entails insufficient continuity and demands quick results.
- The economic strength founded on a philanthropic culture and tax benefits for donations to think tanks.
- The meaning of, in comparison to the rest of the world, the unique rules of confidentiality in this specific security political related area, which permit think tanks to use the same qualified information in their assessments as do the governmental agencies.

Six substantive questions were asked to all respondents. (A summary of the questions posed and the aggregated responses, as well as the full account of the respondents comments can be found in Annex 1 and 2 at http://bit.ly/YhXY1v.) The research question is: *Why and How ''the Big Five'' think tanks mentioned earlier, gain influence?*

INTERVIEW[32] SUMMARY OF IN-DEPTH RESPONSES: THE WHY

Of the six substantive questions asked to all respondents, the most significant responses to the five ''why'' questions are considered here;

The first set of questions focused on the five most highly-ranked think tanks: Please state the reasons why you think that these think tanks are more influential than other organizations? What is it that separates and makes them better than their competitors?

In response to these questions (see Table 1), the emphasis was on the high standard in terms of reports/studies, objectivity (16/18) and independence, networks—especially toward the administration (''revolving door''—13/18)—and a good positioning (i.e., either a niche strongly towards a specific set of questions—seven responses or, as the larger think tanks, the possession of qualitative skills for dealing with a wide range of issues). Several comments

Table 1. Highlights of the Survey on Think Tank Influence

Reason	Times mentioned
1. Why are these five think tanks more influential?	
Network/revolving door	13
Quality of products	11
2. Which values and policy platforms are more likely to gain trust and/or influence?	
Objectivity/courage	16
Reputation	12
3. Which issues or areas are more open to input from academia and think tanks?	
Regional questions—China, Middle East, EU, etc.	12
Strategy formulation—transatlantic relations, UN, etc.	10
4. Successful strategies and tactics?	
Niching	10
5. Failures of strategies and tactics?	
Numerous incorrect judgments/poor quality	9

touched upon the think tanks themselves, and what aspects separate them from the rest in terms of their capacity, abilities, and products.

Having a good reputation for quality of their products (11/18) and balance in what think tanks produce ranked highly among the respondents. One respondent noted that ‘‘they have long established reputations for many years and they produce high quality work and have high quality people’’ (R3, 13-04-2012, telephone). An established track record was an important factor for a few of interviewees (6/18). The issue of the ‘‘revolving door’’ arose on a number of occasions, among the comments on the issue were:

> Three reasons: the first is that they have resources; they have more resources than other institutions. The size, they are much larger and cover a wider variety of topics. And then third, perhaps most important, is that they are able to capture a very senior level of former government people. (R9, 17-05-2012, Skype)

> I think the staffing tends to be pretty dynamic. In particular, when administrations change, there is always a move—seems to be a move—from think tanks into government and government back to think tanks. (R3, 13-04-2012, telephone)

> The thing about RAND that is interesting is that it is a kind of a holding tank for people who are rotating through the government. People will take a job at RAND and then when the party that they are aligned with comes into power they go back into government, and usually at the appointment level. (R4, 16-04-2012, telephone)

Staffing was an important factor for nearly half of the respondents (8/18) in two ways: one, to attract senior staff that possess a high profile and a good reputation, and at the lower levels of staffing, different factors are at play—generating new ideas, being energetic, and "hungry." These people give energy and drive to a think tank. The revolving door was important for two main reasons: to circulate staff between the think tank and government (hence developing a knowledge of government practice and influence) and to expand the network of individuals within the think tank. The size of an organization and its access to resources were also considered important.

The second set of questions focused on issues of trust and influence: Please state which values and policy platforms expressed by think tanks are more likely to engender trust and/or influence within U.S. security policy. In your opinion, how large is the role of reputation and brand in levering influence? Are other factors more important?

Respondents to these questions indicated that reputation, though undefined, is extremely important (12/18). The main factors were objectivity and independence ("no extremists") in the reports and in the personal behavior of the representatives at various events (16/18). Several respondents noted that the successful think tanks are in the "mainstream" with views based on the U.S. Constitution's values. Some expressed the opinion that personnel should be in agreement with basic U.S. values for security policy and related interests, but might perhaps agree to disagree on how to achieve them. Examples included:

> I think with the exception of CNAS, which is rather new, the others have been around for a long, long time. And the fact that they have been around for a long time I think is an indication of the quality of their work, the reputations of the people that are on the staff of those think tanks. So when you put together top notch people and they turn out really, really good, insightful work that influences policy that means that they are going to be around for a long time. CNAS is the only outlier to those five because they are so new, and the fact that they are up there in that top group is an indication that they aggressively want to get really, really good people. (R11, 25-05-2012, telephone)

> Presence in DC—otherwise no impact; Non-partisan (CFR, CSIS, Brookings); Independent—especially on funding; Liberal/centrist values; Pro-free trade ("non-extremist"); Thoughtful conclusions. (R5, 26-04-2012, Skype)

Many respondents referred to the importance of networking, brand, and reputation (12/18) in attracting attention and getting the think tank to the "doorstep" of policy influence. Brand and reputation were seen as influenced by such factors as staffing, product quality (5/18), and organizational longevity. They emphasized that offering a good quality product was necessary for a think tank to get any further: ''The networking and reputation may get you in the door. But if you do not have product you cannot do anything once you are there'' (R3, 13-04-2012, telephone). Brand was construed by several interviewees as being the recognized products of a think tank's staff. Those without professional quality products run the risk of having their brand and reputation damaged, perhaps permanently.

The third set of questions explored the issues and topics that were open and closed to think tanks: Within the security policy domain, are there specific issues or areas that are more open—or closed—to input from academia and think tanks? If so, please state which issues and areas, and why they are more—or less—accessible to influence?

In reply to these questions, regional issues—China, Pacific, Iran, Russia, Europe, the Middle East (''Arab Spring'')—dominated (12/18), as did matters concerning strategy formulation (e.g., transatlantic relations and UN policy—10/18). Functional threats, such as cyber (6/18), non-proliferation, and defense formation (4/18), were also mentioned. Some noted that think tanks having qualified expertise, known to the political administration (the ''revolving door'') and individuals who know where to find relevant information (4/18), receive more opportunities to increase their influence. This aspect was mentioned because most administrations do not have the time or expertise to think long-term in these areas. Similarly, area ''stakeholders'' in Congress or in the administration (2/18) are relatively few.

Think tank policy areas less likely to achieve influence concern bilateral relations with different countries and issues connected to domestic politics. Examples include the question of Israel (5/18), Saudi Arabia relations, materials procurement, and ''privacy'' issues related to Homeland Security. Also, classified areas, such as intelligence questions (5/18) and operational war planning (4/18), are seldom engaged in by the institutions themselves, although staff experts can be contacted on an individual personal basis. Responses included:

> Generally speaking, I think that regional issues tend to be more open to influence and more open to input from academia and the think tank area than the more functional issues. US policy toward the EU, US policy toward Turkey and its initiatives [...] Climate change or currency development [...] or trade [...] those are functional issues, those are everyday as open as regional issues. But there are more functional issues like intelligence and counterterrorism [...] A lot of people will pay lip service to what think tanks say on counterterrorism, but the fact of the matter is the government creates its policy in a vacuum in terms of intellectual contribution. (R2 09-04-2012, Skype)

> I think strategy formulation is more open to influence than is strategy execution. (R3, 13-04-2012, telephone)

> Well, Arab-Israeli conflict issues. For example, if a think tank is going to produce a study that is very critical of US allies, they will not want to hear about it. Like Israel. (R14, 26-06-2012, F2F)

Areas related to intelligence and defense, often requiring a security clearance, are somewhat restricted. In addition, some no-go areas exist, among them criticism of key allies such as Israel (described by one respondent as "the kiss of death"). However, another respondent (R17, 03-07-2012, Skype) noted that think tanks are open to considering almost anything, with the primary factor being the ability to locate a funding source for the project. Respondents also noted that issues defined as being hot and/or sensitive tended to change over time and administrations.

The fourth question dealt with identifying strategies and tactics used by think tanks: What strategies and tactics are likely to bring success for a think tank seeking to influence security policy? Please state any examples of good practice that illustrates this point.

This question identified the role of "niche" as having the highest importance (10/18), defined as either having a sufficient breadth of expertise to make cross-sectorial studies (CSIS, Brookings, CFR, RAND) or to focus on such specific policy-relevant subjects as cyber (ACUS) or COIN (CNAS). Quality of personnel (8/18), with a mixture of senior high-profile individuals and skilled younger and fearless researchers, is also considered a success factor. Likewise, access and networking are ranked high, followed by speed and relevance, so as to not fall behind in the "important" issues of the day—(4/18), as well as governance and proper funding (3/18).

> Well, a first thing is having high profile leadership, no question about that. Secondly, having a board that consists of people who are either very rich or well connected to the government or both. Okay, you go into CSIS's board room, you see the names and pictures of the board, those are two critical elements. High profile leadership and an essentially high profile board allow them to raise more money, it allows them to do government work if they want to, and that gets them going. Now, some think tanks are more media oriented than others. (R6, 09-05-2012, F2F)

> Building relations with government [. . .] Get a reputation through hiring senior government people. Be agile, timely and relevant. [. . .] All top five [think tanks as good examples of this]. (R5, 26-04-2012, Skype)

One of the identified areas was the need to create an environment that encourages people from industry, government, and academia to meet face-to-face at specific events that provide an atmosphere for highlighting products and ideas as well as networking. Both areas have been earlier noted as being essential for any potential influence by the think tanks on governmental policymakers. Being able to move staff between think tanks and government gives another edge in the influence stakes.

Tangible and useful products in hardcopy are still seen as relevant. These products need to be able to grab the attention of a target audience by being new and innovative. According to a few interviewees (4/18), the format should be both visually attractive and concise. Several respondents mentioned the need for a think tank to have a presence in today's social media (though not excluding traditional mass media, such as print and broadcast) in order to attract attention to what it does and can offer to a potential customer.

The focus of the fifth question was to identify sources of possible failure to influence security policy: What strategies and tactics are likely to result in failure to influence security policy? Please state an example of such a case.

In terms of ''fatal'' errors and paths to failure in the fifth question, the responses were somewhat mixed, but highlighted were repeated errors of assessment (9/18), as well as too narrow perspectives (5/18) that result in unrealistic outcomes. Lack of stamina on certain subjects/issues was also emphasized.

> Yes, being spectacularly wrong. But you have to be spectacularly wrong in close proximity to whatever is being proved wrong. [...] Getting it wrong over and over again. There are many examples of being on the wrong side of an issue that no one agrees with you on, if you cannot find any constituency to believe in your ideas you are not going to have any influence. (R2, 09-04-2012, Skype)

> Focusing on yesterday's issues, not recruiting new blood at the highest level. Being excessively national and not having an international reach, I think is important. The big guys all have international advisory boards of one form or another. [...] So you have to have an international reach and if you do not you are going to fall behind. (R6, 09-05-2012, F2F)

> Exactly, indiscretion. Lack of reliability in handling sensitive matters. [...] Failure to meet deadlines, that is important especially that there are many issues that are perishable. [...] Delivering a poor quality product, if you produce something that is not up to a high standard, it is going to be one that could harm your reputation, but two, it would fail to influence anybody because they will say I have not heard anything from this. (R17, 03-07-2012, Skype)

These tactical and strategic errors invariably involve a think tank's developing a bad reputation/brand in any one or a combination of areas that ultimately affects its viability and potentially its very survival. Being repeatedly wrong or providing poor recommendations or policy was a negative, as were products that were either faulty or even non-existent despite lots of talk. Also considered a drawback was the failure to hold or plan activities. Also cited, too, was a lack of expertise in key areas or not staying abreast of important developments. Having staff with a poor reputation, due to failure, faulty analysis, or not coming up with new and interesting ideas were obvious shortcomings.

Overall, the values of objectivity and integrity, of both personnel and product, ranked very high among the responses. One respondent stated that maintaining an ideal objectivity and integrity was very difficult in the "real world." Thus, at times a tension seems to exist between the ideal and actual worlds.

In the area of product, the framing of an issue was considered important. Several areas were identified, among them: being objective, the quality of analysis, finding and establishing a niche, being proactive, the speed (timeliness) and relevance of work, providing useable material that supports policy, and presenting new and innovative ideas on problems that the government does not have time to focus on.

When broaching the issue of product and self/institutional promotion, being available for interviews in the mass media and being seen as present and quoted there; being available and accessible to the Congress; creating key events (conferences, workshops, etc.); and the ability to bring key stakeholders together, as well as an early focus on policy formation, together create valuable avenues for think tank recognition.

While these answers provide an interesting variation of responses to the *why* questions, unifying and making sense of this information is necessary in order to generate a clearer understanding of the broader picture. One factor that stands out is the issue of brand—a think tank's reputation and how it is again perceived by officials and policymakers. Reputation and perception are generated by different means, among them consistently the quality of both personnel and products. These factors, both intangible and tangible, are in turn influenced by a think tank's strategies and tactics.

TACTICS AND STRATEGY: THE HOW[33]

The rich trove of information collected from the responses details the considerations and tactics used by think tanks in their drive for influence. Next considered are the different elements that think tanks incorporate in their quest for success. Those identified, in answer to the how questions, are marketing, the role of the niche, channels of influence, and issues pertaining to target audience. The sixth and final question was "How do you think think tanks influence policy?" In this open-ended question, the focus was on quality and objectivity among personnel, as well as in reports and assessments. Some of the comments follow:

> They give policy-makers a forum to speak in and articulate ideas. [. . .] The second way is you actually infuse the policy process with ideas and options, you can provide options, decision makers love options, the more the better, the fewer the worse. [. . .] And thirdly, they ensure influence by providing a justification for directions the administration already wanted to go. (R2, 09-04-2012, Skype)

> I think think tanks very often have the capacity to set the way in which the issues are framed. [. . .] I think that a think tank has the capacity to influence policy through analysis and production of reports. But even if you create a report you know you have to have someone in power to listen. And so that is the most important way that a think tank actually influences policy, by gaining access. [. . .] So much of that access is informal. (R4, 16-04-2012, telephone)

> The product is still more important than the network, as the position of staff director at NSC is much more important than being a senior scholar at an established think tank. [. . .] The most important strategic issue today is how do we deal with an expanding China? (R1, 06-04-2012, telephone)

Think tanks influence policy through a number of different avenues, many of which have already been identified. These avenues relate to the issues of how a think tank manages the areas of personnel, product, and promotion. In terms of personnel, the value of the revolving door aspect was raised by many respondents as a key to being able to influence policy, though one respondent noted that some hold a negative view of the revolving doors having an impact on the important values of objectivity and integrity, although he personally saw no problem with the practice. Having a dynamic staff is necessary, together with some key people to give the organization a higher profile where it matters.

One tactic/strategy used by successful think tanks is marketing, with several different approaches to marketing their ideas and services. Generally, this involves developing the elements of a good brand, featuring the exploitation of personnel and product.

A good quality product that meets (or exceeds) the expectations created by a think tank's talk must be readily available. Respondents assigned many values and attributes to the "ideal" product—objective, realistic, accurate, readily useable (in terms of policy), timely, innovative, non-controversial (for example, not criticizing key allies), and compact (not overly long).

Personnel are a think tank's cornerstone. Its board and chief executive officer (CEO) need to be known and recognized in government circles;

they need to be proactive and good networkers, and have good reputations for the quality of their work.

Marketing involves using these attributes to gain attention, then recognition, and finally leverage. One point made by the interviewees was that think tanks needed to be physically located in Washington, DC, in order to stand a better chance of influencing policy.

The promotion and marketing of ideas is carried out by different means. Drawing attention from the media is one method, but creating key events that attract important people from government, industry, and academia—such as conferences and task forces—is also beneficial. These provide an opportunity to show potential customers what the think tank has to offer. They also provide an environment for networking to take place. Although one respondent noted that product trumps networking, these activities should be seen as complimentary and not exclusive.

Niche, another tactic/strategy used by think tanks to become successful, is important process-wise at the policy stage and in terms of subject, for example: ACUS on cyber; CSIS on cyber but all-round; CFR on foreign affairs, the UN system, the transatlantic link; Brookings on China and Russia; CNAS on defense policy and military doctrine, such as ''the surge.'' A ''hot'' niche area at the moment is China's expansion in the South China Sea and how the United States could/should respond to this development. Successful niche positioning is developing expertise in areas that the government has neither the time nor the resources to cover.

As for policy influence, think tanks were urged to consider entering the process at an early stage in order to stand any chance of impacting the process. This is related to the issue of framing and discussion of a particular issue, with the window for influence closing after the frame has been established, thereby limiting the allowable parameters of the discussion. Being able to influence the framing of an issue, and therefore how it is viewed and discussed, should lead to a greater opportunity of having some impact upon how policy is formulated.

Additionally, newcomers, both institutional and individual, were advised to focus upon two or three different issues in order to develop a good reputation or brand in those areas, thereby gaining recognition for the quality of their work in those chosen fields. Think tanks that are new entrants in a competitive field are unlikely to have the financial resources or sufficient personnel to undertake a large scale and broad research program, and should therefore narrow their focus and develop a special area of expertise.

Different channels of influence are likewise used by think tanks to become successful. Traditional reports, seminars, television commentary, and quick events for media are part and parcel of getting a think tank's message out to potential customers and to differentiate itself from competitors. Apparent from interpreting several of the responses is that the different channels are not mutually exclusive. Rather they are mutually reinforcing, where one channel affects another and the various links help increase a think tank's potential influence. One response exemplifies this idea:

> [...] being in those three [academia, government and industry] your brand will increase [...] your activity networking, but also the quality of your products and your funding will increase too because many people will see you as a compliment for influencing policy and this will give you more money accordingly and the more money you have the more you can do all those things that attract money and attract influence and attract other activities. It all boils together, blisses together but I think the three elements of the strategies [events, scholarship and revolving door] are obviously solid, and continuing and lots and lots of scholarship both internally and externally through task forces and conferences. (R2, 09-04-2012, Skype)

The ability to exploit channels of influence is enhanced by the think tank's perceived reputation and brand among potential customers and end users. A good reputation and brand will "speak for itself." One channel of influence repeatedly identified by respondents was the "revolving door." Not only does it give a think tank an expanded network, but perhaps just as valuable, it provides actual government experience and is no longer deemed too "academic" and unable to produce useable product.

Moreover, the target audience is also important in becoming successful. Respondents noted a tendency among think tanks of not trying to directly influence policymakers, since doing so is difficult, in terms of access to them and the limited amount of time available. Instead, the tendency now is to target the lower levels of government, such as congressional staff and bureaucrats. They then become potentially a conduit for the think tank's ideas and recommendations to the policymakers. This approach is done through attention grabbing in either social or mainstream media or both, publishing reports, or being in a physical location for "elevator meetings," a very short and concise meeting where a think tank representative can quickly elaborate on what it has to offer in terms of ideas and recommendations.

THE VALUE OF VIRTUE

The premiere characteristic of a successful think tank seems to be credibility based on networks, objectivity, and integrity. An obvious reason for this was offered by Geoff Mulgan, describing the conversion of political access into money, money into ideas, and ideas into legitimacy. Networks open the possibility for political access, but brand and reputation cement those links. Another reason for the indirect approach, as opposed to direct lobbying, is the non-profit status of think tanks that constrains their strategy and tactics. Failure to do so runs the risk of losing this tax status. Likewise, a successful think tank must not be seen as ''extreme,'' but generally as ''centrist,'' with access to both Democrats and Republicans. Next is the academic quality of its reports and studies, as well as the professionalism of its staff. This quality refers to a balanced combination of active young university graduates and more senior individuals who know what decisionmakers need and where the information is available, and being able to ''open doors'' to the closed rooms of decisionmaking.

Thereafter comes the role of positioning and niche so as to maintain a continuously high level in a number of areas that allow a think tank to have access to comprehensive expertise in-house or close-by. Alternatively, a think tank may invest in certain areas where it wants to develop a specialized competence (e.g., ACUS on cyber, CNAS on COIN), notably in areas where the government lacks a sufficient capacity.

Reponses related to the ''how'' equation include the networking factor, mainly between the administration and the think tank (''revolving door''), wherein slightly more senior individuals ''go into exile'' in a think tank and await an administration of the ''correct'' political color, as well as providing opportunities for the personal career ambitions of young talents who await being recruited. The practice provides the chance for individuals in the ''revolving door'' process to expand their networks and gain insider contacts.

An additional important factor is a ''market feel,'' with the flexibility, proactivity, and adaptability to be able to quickly produce a report on a relevant problem area. It may be a larger set of questions where an in-depth study spanning over several years is needed or a shorter policy brief for an under secretary of defense who has been summoned to testify in a congressional committee. In addition to accurate and attractive products, a good communication strategy that balances appearances in the media with other activities such as seminars, report releases, games/workshops, and individual briefing are included here.

A final factor is adequate and long-term financing by individuals and institutions that do not seek to or cannot affect the products' conclusions and the employees' judgments. The ability to convince financiers to provide funds as well as maintaining a good brand are ways of measuring a think tank's success. The head of RAND, Michael D. Rich, describes his firm's three-stage model[34] in which the research agenda is evaluated annually. The first step is whether the research results are of high quality and objective, which is a necessary but not sufficient requirement. The second step is, therefore, being to quickly deliver study results to policymakers and to the public. A think tank becomes satisfied only when it can determine that the right people got the information, and that the decisionmaking processes and policy were directly and perhaps decisively influenced.

The conclusions perceived after the first round of interviews on the role and influence of think tanks have been further substantiated here, as has above all Murray Weidenbaum's thesis about the indirect influence of the network and the "revolving door." Also demonstrated has been that think tanks have a special role to play in the U.S. constitutional arrangement with its lack of a European parliamentarianism and Continental party system, meaning that legislators are generally in greater need of information from outside. The think tanks studied here definitely fill a role as knowledge banks and "lubricants" in the security policy decisionmaking machinery. The increasingly tightening requirements on governmental departments and agencies, combined with more widespread and complex assignments that encounter a lack of expertise for qualitative and long-term assessments, leads to a relatively larger market for think tanks.

Some companies, such as Google, are trying to create think tank-like sections in an attempt to participate in the public debate. But a cursory assessment indicates that they probably never could complete successfully with the mystique, breadth, and quality of the "Big Five"—or even the think tanks further down the list. CNAS—which established itself in six years and within a niche, which according to some respondents became an empty shell when the Obama administration took several of its renowned staff. Becoming successful is a long-term effort, which, without misjudgments and scandals, generally takes between 30–40 years to achieve.

This study, based on unique interviews with very senior and seasoned insiders, will hopefully provide greater appreciation—especially in Europe—of the important and often not fully understood role of think tanks in the U.S. security policy process.

REFERENCES

[1] Lars Nicander, "The Role of Think Tanks in the U.S. Security Policy Environment," *International Journal of Intelligence and CounterIntelligence*, Vol. 28, No. 3, Fall 2015, pp. 480–501.

[2] Geoff Mulgan, "Thinking in Tanks: The Changing Ecology of Political Ideas," *The Political Quarterly*, Vol. 77, No. 2, April–June 2006, pp. 147–155, at p. 148.

[3] R. Kent Weaver, "The Changing World of Think Tanks," *P.S.: Political Science and Politics*, No. 22, September 1989, pp. 563–579; Geoff Mulgan, "Thinking in Tanks: The Changing Ecology of Political Ideas"; Murray L. Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks* (New Brunswick, NJ: Transaction Publishers, 2011).

[4] James McGann, *The Global Go To Think Tanks Report 2011*, University of Pennsylvania. The U.S. tops the list with 1815 think tanks, followed by China with 425, the United Kingdom with 292, and Germany with 286.

[5] Richard Higgott and Diane Stone, "The Limits of Influence: Foreign Policy Think Tanks in Britain and the USA," *Review of International Studies*, Vol. 20, No. 1, January 1994, pp. 15–34; Murray L. Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks*.

[6] Donald E. Abelson, *Capitol Idea: Think Tanks and US Foreign Policy* (Montreal: McGill-Queens University Press, 2006).

[7] R. Kent Weaver, "The Changing World of Think Tanks."

[8] Murray L. Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks*.

[9] Eric Swank, "Clinton's Domestic Policy Makers: Big Business, Think Tanks and Welfare Reform," *Journal of Poverty*, Vol. 2, No. 1, 1998, pp. 55–78.

[10] Among the independent agencies are the Central Intelligence Agency (CIA), National Reconnaissance Office (NRO), National Security Agency (NSA), Defense Intelligence Agency (DIA); also involved are the Defense Advanced Research Projects Agency (DARPA), United States Coast Guard, Federal Bureau of Investigation (FBI), and the foreign affairs, armed services, and intelligence committees in the Congress.

[11] Murray L. Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks*, p. 58.

[12] R. Kent Weaver, "The Changing World of Think Tanks," p. 564.

[13] *Ibid.*, p. 567.

[14] Murray L. Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks*; and Geoff Mulgan, "Thinking in Tanks: The Changing Ecology of Political Ideas," p. 148.

[15] R. Kent Weaver, "The Changing World of Think Tanks," pp. 568–569.

[16] Geoff Mulgan, "Thinking in Tanks: The Changing Ecology of Political Ideas," p. 148.

[17] *Frequently Asked Questions*, Gateway House, Indian Council on Global Relations, at http://www.gatewayhouse.in/about-us/how-you-benefit/faq/, 27 April 2010. Accessed 10 September 2014.

[18] *What is a Think Tank?*, NCPA, at http://www.ncpa.org/pub/what-is-a-think-tank, 20 December 2005. Accessed 10 September 2014.

[19] *Exemption Requirements—501(c)(3) Organizations*, Internal Revenue Service, at http://www.irs.gov/Charities-&-Non-Profits/Charitable-Organizations/Exemption-Requirements-Section-501(c)(3)-Organizations, 13 March 2014. Accessed 10 September 2014.

[20] Eric Lipton, Brooke Williams, and Nicholas Confessore, "Foreign Powers Buy Influence at Think Tanks," *The New York Times*, 6 September 2014, at http://www.nytimes.com/2014/09/07/us/politics/foreign-powers-buy-influence-at-think-tanks.html. Accessed 8 September 2014.

[21] Lars Nicander, "Shielding the Net—Understanding the Issue of Vulnerability and Threat to the Information Society," *Policy Studies*, Vol. 31, No. 3, 2010, pp. 283–300.

[22] R. Kent Weaver, "The Changing World of Think Tanks," p. 570.

[23] James G. McGann, *Think Tanks and Policy Advice in the US: Academics, Advisors and Advocates* (New York: Routledge, 2007); James G. McGann, *2012 Global Go to Think Tanks Report and Policy Advice* (Philadelphia: University of Pennsylvania, 2013); James G. McGann and Erik C. Johnson, *Comparative Think Tanks, Politics and Public Policy* (Northhampton, MA: Edward Elgar Publishing, 2005); Andrew Rich and R. Kent Weaver, ''Think Tanks in the US Media,'' *The Harvard International Journal of Press/Politics*, Vol. 5, No. 4, 2000, pp. 81–103; Andrew Rich, ''US Think Tanks and the Intersection of Ideology, Advocacy and Influence,'' *NIRA Review*, Winter 2001, pp. 54–59; Murray L. Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks.*

[24] John W. Kingdon, *Agendas, Alternatives, and Public Policies*, 2nd ed. (New York: Pearson, 2011), p. 54.

[25] The non-profit RAND encompasses three Federally Funded Research and Development Centers (FFRDC) of which RAND's National Defense Research Institute (NDRI) is the most important here.

[26] Council on Foreign Relations, *About CFR,* available at http://www.cfr.org/about/Council on Foreign Relations. Accessed 16 December 2013.

[27] The eighteen respondents—interviewed through personal meetings, through Skype and by phone—have been renamed to R1 through R18 because of confidentiality issues, quotes from all respondents have not been used to highlight claims in this article but have naturally been taken into consideration.

[28] Jack H. Nagel, *The Descriptive Analysis of Power* (New Haven, CT: Yale University Press, 1975), pp. 29 and 55.

[29] Murray L. Weidenbaum, *The Competition of Ideas: The World of the Washington Think Tanks.*

[30] Colin S. Gray, ''Think Tanks and Public Policy,'' *International Journal*, Vol. 33, No. 1, Opinion and Policy, 1977–1978, pp. 177–194, at p. 177.

[31] Erik Voeten, ''What do Policymakers Want From Academics?,'' at http://www.washingtonpost.com/blogs/monkey-cage/wp/2013/09/25/what-do-policymakers-want-from-academics/, *The Washington Post*, 25 September 2013. Accessed 29 September 2013.

[32] There is limited space here for a complete discussion of all that was said, a summary is provided. Please see on-line Annex 1 for an overview of the different answers given by the respondents and Annex 2 for additional quotes from the interviews.

[33] Please refer to the final section of Annex 1 for the alternative quotes given to this question.

[34] Allen McDuffee, *Q&A with Rand Corp.'s Michael D. Rich: 2012 elections, Syria and toxicity in Washington*, at http://www.washingtonpost.com/blogs/think-tanked/post/qanda-with-rand-corps-michael-d-rich-2012-elections-syria-and-toxicity-in-washington/2012/08/06/eacaf1f2-dfbb-11e1-8fc5-a7dcf1fc161d_blog.html, *The Washington Post*, 8 June 2012. Accessed 16 December 2013.

C. Summary & Conclusions

1. Findings

The research question posed in the introductory chapter concerned an investigation of the overall decision-making process in all phases of the analysis model (A + B + C), as well as indicating the bottlenecks for non-time critical threat developments. The assumed basis for an ideal process could be illustrated as in the box below.

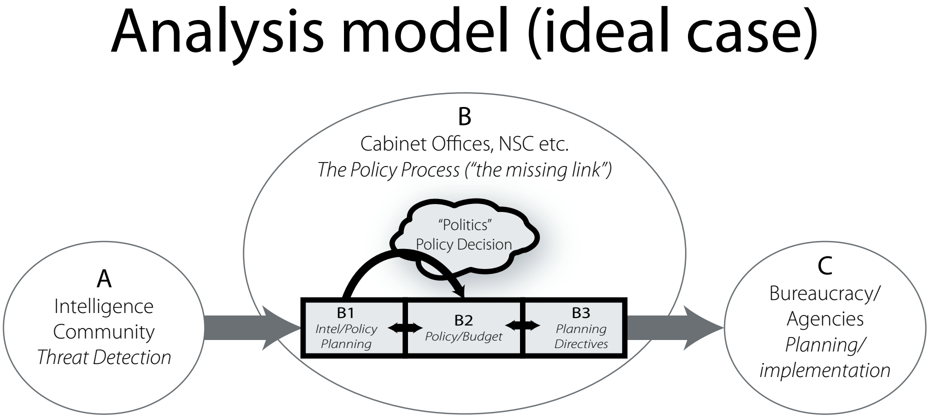


Figure 6: Ideal Case

1.1. Article 1

This article looked at the policy processes of a number of different countries, from the point of realisation that a problem needs attention to the implementation of government policy. The event that initiates and drives the reform process of each country is tracked, revealing differences and similarities in urgency and perceived risks in the task of overhauling the legal framework for Critical Information Infrastructure Protection (CIIP). The final part of the article sought to understand and account for those similarities and differences in policy implementation or in some cases, the lack of it.

The findings suggested that certain lead countries that initiated the process of policy reform in CIIP caused a number of other countries to follow suit, which was a form of transnational policy "bandwagoning." Although there were similarities in the trigger mechanism which initiated the process, there was divergence in the passage of the recommendations and policy suggestions due to the structure of the national governments and bureaucratic structures that placed constraints upon the progress in some cases.

The analysis revealed a number of cases, which showed compromises and other strategies in an effort to push the reform through in a contested political process, and where cooperation from government agencies was not necessarily forthcoming. Some of the reform processes have even stalled and were in a form of limbo, a position from which they have not been able to gain any momentum.

With the apparent fact that there was a difference between countries in this aspect, the final finding was that the top politicians own the policy process, whilst the bureaucracy/administration owns the implementation component.

1.2. Article 2

The purpose of this article was to investigate how Intelligence Communities innovate (adaptability) and how new demands of pluralism in the intelligence production process have been fostered. By innovation, it is specifically referring to how the intelligence organisations and the legal/political machinery in the sector evolve to meet the changes and challenges found in their environment.

The lessons drawn from organisational learning demonstrated that the policy process of bringing about innovation and change was not necessarily a rational one that applied to best remedy the identified problem or error. It revealed a process watered down by bargaining and politics, especially in a sensitive field as intelligence. A number of other factors in the organisation and the state which it serves also played a part - personal, "culture" etc. within the Intelligence Community - together with their interests and biases.

The finding here was how the intelligence part of the decision chain (A + B1) functioned and developed in an environment of closed knowledge monopolies, normally also in the absence of external competition and pluralism. An important advantage with the American intelligence system seemed to be that pluralism and adaption was relatively large in comparison to the rest of the world. However, there is then on the "flop-side" a risk with the American system of making rapid and hasty organizational decisions, such as creating new organizational layers on top of an existing structure.

1.3. Article 3

Article 3 focused on which terrorist organisations might become the first actor to use information weapons in their warfare, such as attacking the vulnerabilities of modern information society and how the intelligence community (A) could detect these quickly unfolding attacks in light of the complex nature of their bureaucracies, which might make such early detection difficult. The article illuminated the complexities of understanding a potential leap towards convergence between terrorism and cyber warfare and it offers a potential roadmap towards the necessary measures to bolster investigative and enforcement mechanisms within the international community.

Here a practical showcase of how a possible new threat phenomenon with anonymous information/cyber-terrorists may be assessed, in which it is not enough to only assess a threat actor's intentions and capabilities, but they should also be coupled with societal vulnerabilities. This knowledge is not always available within the intelligence community, but can be found at the operational level of relevant governments and private businesses. The ability to think in new ways and "outside the box" instead of "inertial navigation" is discussed.

1.4. Article 4

This article focused (with a Swedish perspective) on the sometimes blurred concept of information operations, which to a large extent can be considered as a mirror image of the increased dependencies on electronic information, networks and IT systems in modern civilian societies. The article discussed the weaknesses and strengths of an ever growing expansion of these networks for the sharing of information, and how to implement new cross-sector cooperation to fully adapt to new preparedness measures in the bureaucracy.

The article further described the process and indicated bottlenecks (B3 + C) foremost on the agency level based on the same scenarios of IT threats as the initial comparative study in Article 1. The proposition that the policy process is not able to balance the bureaucracy's "centrifugal forces" is confirmed and deepened by this empirical case study within a Swedish context.

1.5. Article 5.1 and 5.2

Finally, the two contiguous articles 5.1 and 5.2 dealt with the special case of the United States in relation to several other countries, in which think tanks have a special role concerning cultivating pluralism in security policy decision-making, as well as being a disintegrator of knowledge monopolies. The way that public policy is formulated has been changing. What had been a governmental domain has opened up to the input of other external actors – with public policy Think Tanks exemplifying the significant roles that private sector actors can play in this sphere.

The first article 5.1 explored how think tanks influence the policy process. On the one hand, there are theoretical explanations that have been offered by the academic community. On the other hand, this is how practitioners view the issue. Therefore, this article seeks to expose a greater level of understanding of this influence through comparing and contrasting these two broad conceptual camps. A theoretical overview was provided, which was complemented by the distribution of a questionnaire to experienced practitioners. The United States was chosen as the case study for two main reasons. The greatest concentration of think tanks is found there as well as the differences in the traditions of government which allows for external actors to contributing to the policy process. Under such conditions, if Think Tank influence can be discovered and therefore the ability to analyse it, this is the best place to look for it.

The second article 5.2 dealt with how think tanks were able to gain success in influencing the security policy process in the United States. Success was understood as the ability to influence at some stage and in some manner the policy process – anywhere from identifying a "problem" or opportunity to implementing policy. Therefore the focus was on the why and how questions affected the issue of influencing policy. A valuable and unique insider perspective was also provided by the extensive material collected from the experts who responded to the dissertation's survey, which contribute to developing the understanding of how think tanks gain influence in policy in countries such as the United States.

1.6. Conclusions of article findings

Observations regarding factors that shorten the timeframe of decision-making processes (A + B + C) can already be seen in the comparative study in Article 1 – namely, countries with homogenous management and ministerial rule (e.g. Australia) seem to have shorter decision-making timeframe processes. In particular, the so-called spoil system in the United States, in which thousands of top executives in management are appointed for short terms of office, seems to promote a fast decision-making process, perhaps sometimes at the expense of substantive expert content. This is one of the reasons why think tanks function as a lubricant and knowledge complement in the American environment, at least in the best case scenario.

The identified problem of why the bureaucracy has too much room for interpretation in relation to the policy process was discussed in the introductory chapter. One of the findings is that savings on the government office level can lead to excessive outsourcing of the governing planning function (B3) to agency level.

On the threat side (A), Britain also has certain pluralism regarding intelligence assessments as they have a tradition of systematically and discretely collecting assessments from trusted academics within the British academic community on an individual basis, such as the tradition of "Oxbridge" as a component of the British "ruling class." In recent years, other countries' intelligence services have also begun to engage in alternative scenario activities, however, this leans towards "foresight" as it involves cases of longer time horizons of 15-20 years, with such studies requiring extensive academic input.

Otherwise, the decision-making systems are relatively closed in the area of security policy, and it is not only due to tradition and the constitution. Even though most agree that pluralism is important for the process, the majority of the countries do not have a wealthy economy on the scale of the United States that can fund this process. Too much pluralism can also be costly and lead to problems in balancing efficiency-confidentiality considerations, as well as the need, at times, for quickly produced advice.

The assumption in article 1, that the major problem in the decision process (A + B + C) is the connection between the policy process and bureaucracy (B + C), can be qualified by taking into account the relations within the policy sub-processes (B1 + B2 + B3). It was observed, especially in small Cabinet Offices the planning function (B3) can become a voice of the strong and independent agencies, making the policy impact go "upstream", which might increase the tensions between B2 (policy making) and B3 (planning direction) when thinking in terms of incrementalism, as opposed to making major changes in policy direction. The most important link is between B3 and C (the bureaucracy) as this concern directing the planning at the agency level so that policy decisions are implemented as intended.

In summary, three conclusions are proposed in this dissertation based on the overall observation that the "Knowledge Monopoly" and lack of transparency and "second opinions" are the main variables preventing better seamlessness between the threat and planning communities. Firstly, the main inertias found in the closed innermost core of the state apparatus seems to be lack of horizontal communication and transparency as well as contradictory bureaucratic interest when it comes to implementation. These hardly modify on their own due to introversion and knowledge monopolies. Secondly, this relationship has received relatively little attention from academics and the research community at large, due to accessibility difficulties among other issues. Thirdly, the employment of the Think Tank model in these processes, in certain circumstances, may be a means to reduce such inertias.

Three sub-questions that were posed in the introduction, which require further attention. To restate these three questions:

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

Security policy threats have, and continue to, evolve at a very rapid pace. Perception plays a significant role too. There is the need to for planners and policy makers to clearly distinguish between the strongest and most capable source of threat and the threat that is most likely to occur. For example, Russia has a significant military potential, but the probably of it being used against the United States in a direct military conflict is less than the militarily weaker terrorist organisation ISIS. The threats have moved from an environment of a more predictable state-based origin to rapidly evolving non-state based threats (such as cyber security, and a plethora of transnational terrorist organisations). Some of these threats can easily cross borders, such as the recruitment of Western citizens by ISIS, which creates risks within Western countries as witnessed by the numerous terrorist attacks committed in European countries (such as the murder of the soldier Lee Rigby in Woolwich, England).

These threats can stimulate innovation and change in government bureaucracies, policy formulation and implementation, but this is dependent on a number of factors. One of these is perception and awareness among policy makers and the bureaucracy. If they are not aware or the issue is a low political priority or politically overly sensitive, it may not receive the require attention and measures to redress the situation.

Cyber has been successful in gaining attention and priority around the world, it is a high probability and potentially high impact risk faced by most countries, and therefore a great deal of time, effort and finances has been devoted to the issue, it is also perceived as being an immediate risk in the here and now.

Climate change and the means of addressing it have proven to be much more problematic owing to diverging interests among countries, governments, business, academia and the public as well as the perception that it is not an immediate issue as it can projected as being a future threat.

There are a number of observable problems and obstacles in addressing the new threats. Not least among these is the issue of perception. If a problem is not recognised or is seen as something that can be dealt with in the future as there is 'time' available before it becomes critical. Conflicts can also emerge between different stakeholders in the policy environment. The bureaucracy may resist change, given the competitive policy environment the best policy option may not be chosen – rather the one that gains the greatest attention amount of and appeal.

Ideally, a critical ontological turn is needed in order to tease out knowledge from the unknown, in this case on identifying previously unknown and understudied processes, structures and relations within the policy formulating government bodies as the Cabinet Offices.

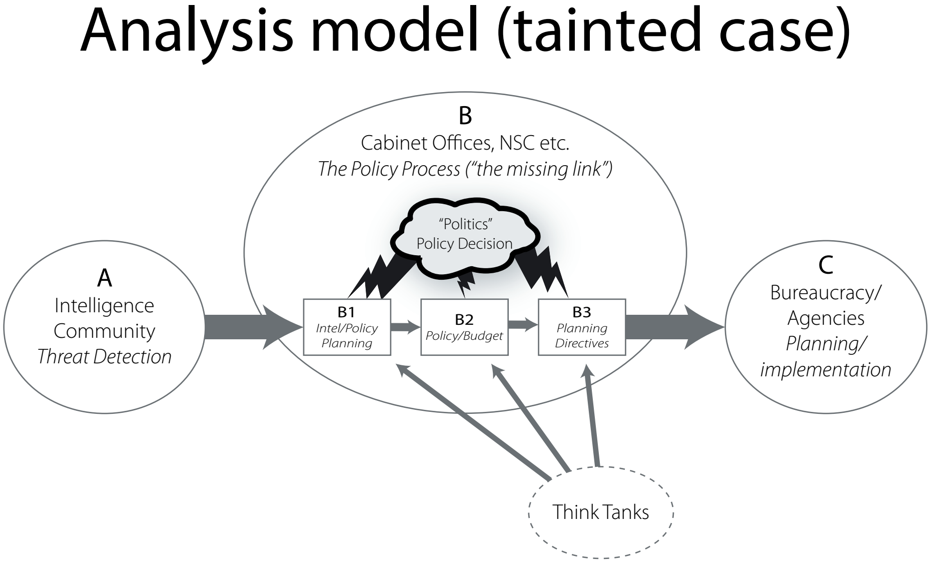


Figure 7: Tainted case

2. Differences depending on policy impact – an alternative case?

The case study in Article 1 that has been the basis for the reasoning about pluralism and knowledge monopolies deals with how critical system threats towards the information society became foundations for planning in different countries protective strategies. This type of threat picture has had relatively little party political overtones as it is understood as a consequence of the "neutral" technical development.

However, if we look at a case in which the condition for the fundamental ideal process is disrupted by distorting inputs from the political level based on predetermined ideas, the process can be quite different. Instead, the adjoining picture can illustrate the above reasoning.

In the United States during the Gulf War in 2003, the traditional intelligence community's assessment procedures were short-circuited as the political leadership in the Pentagon had its own political agenda and acquired their own intelligence cell (Office of Special Plans) which steered the intelligence reporting to fit the predetermined policy objectives. This phenomenon is usually referred to as "cherry-picking", which is anathema to all Western intelligence services credo to provide the most unbiased knowledge and objective decisions that is possible to produce.

In recent years, the Swedish defence policy has, in light of Russia's actions, been put under strong domestic pressure after almost 20 years of constant disarmament. The defence policy also became the subject of unusual and intense public debate during the election campaign in 2014. The background is that disarmament seemed a logical course in relation to the collapse of the Soviet Union in 1991, and influential generals spoke of a "strategic time-out". The parliamentary Defence Commissions that prepared the Government perennial defence decisions worked systematically according to the previous model, in which a coherent and quite seamless decision process was formed and became the model during the entire Cold War. The results were a number of so called secret specified threats used for defence planning purposes in which the Armed Forces planning was directly linked to the updated security policy assessments.

In Sweden there is a current example concerning Russia's assumed geopolitical intentions in relation to events in the Crimea and Ukraine crisis in 2014 which, if converted into the above mentioned analysis model, would generate a completely different policy outcome. Here the political prerogative view that Russia´s intention could not be problematic prevailed too long though warnings from the Intelligence Community. If so, it is not in the relation between the policy level and the bureaucracy (B + C) where the bottleneck is the greatest and the agency level does not implement policy decisions, but the unwillingness from the policy level to accept input from the intelligence system.

Here, we find that the intelligence community (A) warned the policy level (B), but without effect. In this case, the problem seems to be within the policy sub-processes where especially the intelligence process (B1), which receives the information from the Intel Community (A) – and also the planning process (B3) who has managerial dialogue with agency C, does not reach B2 that is responsible for budgetary considerations. B2 – in this case, officials at the

Department of Defence – are subordinate to the political context and the priorities the Secretary of Defence and the Cabinet in general consider trade-offs against other domestic political expenditures of interests.

As the Cabinet Office is a politically steered organization there is no objective requirement that received intelligence assessments and decisions should be connected or coordinated with each other. It may even be that those who manage assessments (B1) dismiss or even signal disapproval of assessments that do not comply with the above mentioned ruling political stance.

In this case, when it comes to a political conceptual perception in relation to official policy it probably would not involve an ideally functioning chain of command, since, as with the first IT case, the bureaucracy would be expected to implement it. The position highlighted in Article 1 – "the politicians own the policy process, but the bureaucracy own implementation" – is confirmed as to why the process gets stuck already at the starting line.

The answer to the research question if, and possibly how, the chain of command can be shortened becomes disappointingly negative in relation to whether it is a politically controversial or loaded question – contrary to, for example, the case of threats to the information society where decisions have to be made in a fast paced environment.

If the result in the comparative Article 1-study is analysed from the point of view of which countries had the earliest start on indicating possible threats against their information society – with an assumed well functioned relation between the intelligence community and the policy level (AàB1) – one might consider the UK system as being exemplary. This is due to the fact that they started their internal policy debate in the early 1990s and took the necessary preparatory steps in response, while other countries like Australia were late starters. Even if this area is touched upon in the article 2, there could still be room for more thorough analysis, nevertheless. To understand these issues, one should refer to the field of Early Warning studies, which is a well-researched area with renowned literature such as Richard Betts (1982) *Surprise attack: Lessons for Defense Planning* and Roberta Wohlstetter's (1962) *Pearl Harbor: Warning and Decision.*

3. The role of Think Tanks

Would the defence and security policy-making process in the case of Sweden have been any different if there had been independent think tanks of American model in order to provide independent knowledge on these issues? Probably not in the concrete example cited above, as the political preconceptions are so radically different from the more objective input values that the intelligence community aims to contribute to the policy process.

The study of the American think tanks role shows in fact that their influence can be quite limited in areas where the political attitudes (e.g. policy towards Israel) are strongly held. These cases are however considered to be specific exceptions in relation to the entire policy environment in which think tanks operate. Rather, it is when it comes to completing objective knowledge gaps, and to evaluate various non-politicized policy options, where the focus of the agency level is clarified, the value and need for pluralism is greatest.

Pluralism in policy making is important, but in itself pluralism is not a complete guarantee for better quality decisions and policy as it is a means and not an end in itself. There are other factors that need to be taken into account. There are dual aspects of the quality of the final product AND the process of getting there. Research and market intelligence should not be compromised by overt or covert political or economic influence over the nature of report results. Such trends have been exposed in recent media exposés of foreign influence of think tanks in America through economic incentives to produce findings that match the expectations of the funders, who may require legitimation of their governments' policies.

The September 2014 New York Times exposé of the Brookings Institution (described in more detail further on) has had a snowball-effect on this one particular illustrative case, which has been taken up as a four part investigative series in America (see, The Investigative Project on Terrorism, 2014). This is indicative of the dangers present in a public policy environment that demands a rapid flow of accurate information in order to make correct decisions, but when there is an element of deception and hidden agenda within those same information flows due to external influences on the researchers.

What are the administrative and legal barriers of introducing a system of think tanks in Sweden and other Nordic countries according to the model above? Firstly, regarding sensitive national security issues, it becomes necessary to change legislation into introducing a system of personal security clearances instead of the current system based on function in which someone holding a particular position in a defence or security related agency obtains a clearance. Thus would have the effect of eliminating formal barriers for access to relevant, but confidential information. This requires changes in political culture and practice, which do not easily change in short time spans, including the desire by researchers to publish their research without government restrictions.

Secondly, changes in economic conditions for think tanks are needed, enabling think tanks to operate and recruit senior and competent personnel offering competitive salaries. To achieve this it requires, as in the United States, a different tax deduction system for donors to enable them to qualify to fund these types of research foundations and non-profit research organizations. This provides prestige and credo to those who provide funds as well as contributing to cognitive diversity in otherwise inaccessible areas. Simultaneously in the last year – after the investigation for this dissertation – concerns are raised that the integrity of even the big think tanks has started to erode, which is an important consideration for Swedish research institutes who desire to maintain their independence, even at the cost of not being funded by major corporations or foreign governments.

4. Afterword

The dissertation has endeavoured to provide different perspectives on the rationality of security and defence policy, in which significant identified threats are neutralised as quickly as possible through the creation and implementation of effective protective measures. As much of the information and planning measures imply security classification of the transparency and debate on these issues, alternative assessments becomes limited. Still, there should be a need to improve the decision-making system and streamlining the state apparatus to become more efficient. The remaining significant question is whether in this line of work it is possible to ignore the fact that there is a political will that is not rationally based that affects the policy making process, thereby limiting the possibility of pluralism in policy making.

One of the shortcomings of this thesis can be found in the methodological approach that was used, which was not conducive to theory development. However, given the relative lack of existing research on the topic of this thesis, a different approach was needed. This is why the multi-disciplinary perspective, as described by Evans and Davis (1999), was used over a single disciplinary approach. It also explains the use of the critical ontological turn, these mechanisms were intended to tease out and enrich the wider implications for further research in this field of study. Although this work may not have advanced theoretical development in the area, it has developed a greater appreciation and understanding of the empirical processes. By developing the empirical basis of research, more accurate and reliable predictive theoretical and conceptual tools can be conceived. This is a gradual process of gaining knowledge from an environment where little existed previously. It is hoped that this thesis may be one of the steps in encouraging further research in this area and thereby creating the necessary conditions for solid theoretical development.

The transferability of the results could also differ between different countries, as indicated in article 1 where governments with ministerial rule seems to have shorter decision-making cycle than parliamentarian countries like Sweden with independent agencies formally adhering only to collective Cabinet decisions.

The cross-sectorial research field that this dissertation touches upon has demonstrated the existence of such under-researched areas. Hopefully this will also have a scholarly relevance and lead to new knowledge within the concept of Policy Transfer Analysis, which bridges at least the three disciplines of Security Studies, Policy Studies and Public Administration. This thesis is at the cross section of these disciplines, specifically how new and emerging security threats are recognised, managed and resolved through creating and implementing public policy. It covers the whole process and all stakeholders – organisations (such as think tanks), government bureaucracy and governments.

One of the greatly under researched areas, which is raised in the above, is the level of covert political and economic influence by external funders on think tanks and the policy process in general. This phenomenon is difficult, although not impossible, to research, and is dependent on the work of investigative journalism. The New York Times article (New York Times, 2014) mentioned earlier scratches the surface and hints at a significant problem that ideally could shake up the system (although, in practice, it is so institutionalized and widespread that it is unlikely to change). There have already been some political reactions to this issue, so a comprehensive and objective academic approach is needed to understand the exact nature and scale of the problem, as a first step on the way to addressing it.

Finally, despite such shortcomings, it might be possible for an improvement to take place in the relationship between think tanks´ and government policy making bodies in the US, with recognition that private sector research institutes still have a role to play in providing independent sources of policy advice to government policy makers.

One outcome in this dissertation is also that of a significant connection between pluralism in the decision-making process on one hand, and adaptability as well as faster bureaucracy implementation on the other. A remaining issue is whether it will be permitted for tax-exempt think tanks to engage in advocacy and lobbying activities – legally and practically. This is an important change to understand owing to the implications concerning the covert influence on policy by external donors – when they might be involved in funding such activities.

More multi-disciplinary research needs to be undertaken in the field of security and foreign policy in terms of the relationship between think tanks and government policy making. Such research should take into account the findings of specific academic disciplines – public policy, sociology, political science … etc. Thus, additional strength to arguments and developing an even wider perspective on these issues can be gained through combining as wide a spectrum of relevant disciplines to exploring how today's significant and pressing national security problems can be solved through effective research, whether in think tanks, government agencies, or through a constructive engagement by these communities.

References

Betts, Richard K. (1982). *Surprise attack: Lessons for Defense Planning*. Washington DC: Brookings Institution.

New York Times (2014). “Foreign Powers Buy Influence at Think Tanks”, 2014-09-06. http://www.nytimes.com/2014/09/07/us/politics/foreign-powers-buy-influence-at-think-tanks.html?_r=0
Retrieved 2014-10-14.

The Investigative Project on Terrorism (2014). “Qatar’s Insidious Influence on the Brookings Institution: A Four Part Investigative Series: Brookings Sells Soul to Qatar’s Terror Agenda”, 2014-10-28.
http://www.investigativeproject.org/4630/ipt-exclusive-qatar-insidious-influence-on
Retrieved 2014-11-07.

Wohlstetter, Roberta (1962). *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press.

D. Sammanfattning

Huvudfokus för denna avhandling är området byråkratisk förändringsbenägenhet i förhållande till omvärldsutveckling på det säkerhetsrelaterade området. Syftet är att från olika infallsvinklar studera samspelet och kopplingarna mellan ett antal statliga nyckelinstitutioner. Dels de som har att uppmärksamma och varna för olika former av antagonistiska hot, dels de strukturer som har att planera för samhällsskyddet genom att snabbt och smidigt omsätta dessa signaler till styrande inriktningar med motsvarande resursallokeringar till utsatta sektorer. Kravet på snabbhet i denna process har ökat radikalt i och med informationssamhällets utveckling och där gårdagens rutiner inte är anpassade till dagens nya hot och sårbarheter. Därför är studier av de mekanismer som kan påverka snabbheten i högsta grad policyrelevant.

Avhandlingen är inducerande med försök till teoridiskussioner om policyformuleringsprocessen (”the missing link”), där konklusioner från de tre huvudartiklarna (1,2 och 5) blir pusselbitar i kappans slutkapitel. Avhandlningen hör hemma inom statsvetenskapens säkerhetsstudier (Security Studies) men med en stark koppling till förvaltningspolitiska områden (Public Policy/ Public Administration), och framför allt den tämligen nya underdicplin som beskriver policyformuleringsprocessen (Policy Transfer Analysis). Ingen idag existerande teoribildning som beskriver incitament för förändring i slutna monopol i statsapparatens innersta kärna har dock ännu identifierats.

Den forskningsfråga som står i centrum är: *Hur kan man tidsmässigt förkorta processen från upptäckten av nya hotförutsättningar till att nödvändiga skyddsåtgärder implementerats, och var finns flaskhalsarna?*

En viktig hypotes som prövas i avhandlingsupplägget är att ökad pluralism – både på hot- och planeringssidan – medför ökad förändringsbenägenhet beträffande att implementera föranledda åtgärder och förändra förvaltningsstrukturer.

Det kan handla om såväl olika militära försvarssystem som civila kritiska informationsinfrastrukturer kopplat till el- och telesystem. Ett särskilt förhållande är att dessa processer till övervägande del äger rum i slutna system med kunskapsmonopol där externa inflytelser (”peer review”, marknadsmekanismer etc.) är närmast obefintliga. Hur påverkas och utvecklas dessa strukturer för ”Hot” respektive ”Planering” av omvärldsutvecklingen? Finns det en ”Missing Link” här i kedjan ”hotupptäckt-policyformuleringsprocess-byråkratisk implementering”? Vad hindrar denna process från att proaktivt och linjärt antecipera nya förutsättningar?

Strukturen består av en övergripande introduktion samt fem artiklar som på olika sätt belyser problematiken och några kärnfrågor. De första två är kortare och mer indikativa medan de tre senare är mer djupgående. Den sista femte artikeln är i sin tur tudelad i en mer teoretisk del och en mer empiriskt inriktad. Ett avslutande konkluderande kapitel försöker identifiera de flaskhalsar

kring denna typ av planering som kan finnas. Även om resonemangen främst tar sin utgångspunkt i ett mindre marknadsekonomiskt och informationstekniskt utvecklat land som Sverige, så sker flera exemplifieringar från USA beroende på den relativa stora transparensen där kring hanteringen av dessa frågor.

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

Lars Nicander

New Threats – Old Routines

Bureaucratic adaptability in the security policy environment

Within the framework of state security, 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.

9 789521 232831 >

ISBN 978-952-12-3283-1