FFI-RAPPORT

19/01766

Defence against foreign influence

— a value-based approach to define and assess harm, and to direct defence measures

Torbjørn Kveberg
Vårin Alme
Sverre Diesen

Defence against foreign influence – a value-based approach to define and assess harm, and to direct defence measures

Torbjørn Kveberg
Vårin Alme
Sverre Diesen

Norwegian Defence Research Establishment (FFI) 11 November 2019

Keywords
Sikkerhetspolitikk
Strategisk kommunikasjon
Informasjonsoperasjoner
Propaganda
Desinformasjon
Totalforsvar

FFI report
19/01766

Project number
1368

Electronic ISBN
978-82-464-3243-4

Approvers
Ole-Erik Hedenstad, *Research Manager*
Jan Erik Voldhaug, *Director of Research*
The document is electronically approved and therefore has no handwritten signature.

Summary

How can states defend themselves against foreign influence? Western states' need for a defence against foreign influence is not new, but it has become more pressing over the past decade. Many will claim Strategic Communication is the answer, but major disagreements remain as to what that is and ought to be. This report details an alternative approach to defence that clearly articulates what it is, and why it contributes to a meaningful defence against foreign influence.

To detail this approach the report looks deeper at what it means to defend against foreign influence, and then investigates how to defend against foreign influence. The report identifies three tasks for defence that any such concept must address:

- Define what constitutes harm.
- Assess what foreign influence harms.
- Describe the objective of defence measures.

The report assumes the purpose of defence is to protect state security, which means state security is central to define what constitutes harm. The report therefore proposes that states take stock of their essential state security interests. A relational model of power is used to hold this information in a manner that is meaningful when considering the threat from foreign influence. This leads to an overview of essential state security interests, where each is expressed (ideally) as a behaviour that is desired from a specific actor. A simple example would be «State A offers and provides military support». The report offers suggestions for how governments can map their interests, and how these can be expressed and illustrated in accordance with a relational model of power.

The overview of state security essentials describes what states value most, which is why the report calls it a value-based approach to defence. With respect to the three tasks above, foreign influence activities that have undesirable effects on these state security essentials are considered harmful. The objective of defence measures is to alleviate that harm. Government practitioners using the approach must therefore select a set of possible foreign influence activities, and assess whether and why they harm any state security essential. The report provides a method called «set generation» to aid in this process.

The report recommends that the value-based approach be further refined and tested.

Sammendrag

Hvordan kan stater forsvare seg mot fremmedstatlig påvirkning? Vestens behov for et forsvar mot påvirkning er ikke nytt, men har blitt tydeligere i løpet av det siste tiåret. Mange vil hevde at strategisk kommunikasjon er svaret, men det er store uenigheter om nøyaktig hva det er og bør være for noe. Denne rapporten beskriver en alternativ tilnærming til forsvar som gir tydelig uttrykk for hva den er, og hvordan den bidrar til et meningsfullt forsvar mot fremmedstatlig påvirkning.

For å beskrive en tilnærming diskuterer rapporten hva det betyr å forsvare mot påvirkning og deretter hvordan stater kan forsvare seg mot fremmedstatlig påvirkning. Rapporten identifiserer videre tre oppgaver innen forsvar som ethvert konsept for påvirkning må løse:

- Definere hva skade er.
- Vurdere hva fremmedstatlig påvirkning skader.
- Beskrive formålet med forsvarstiltak.

Rapporten antar at formålet med forsvar er å beskytte statssikkerheten, hvilket betyr at statssikkerhet er helt sentralt i å definere hva skade er. Rapporten foreslår derfor at stater skaffer til veie en oversikt over sine essensielle statssikkerhetsinteresser. En relasjonell maktmodell brukes til å fremstille denne informasjonen på en meningsfull måte. Det fører til en oversikt over essensielle statssikkerhetsinteresser, hvor hver interesse uttrykkes i form av en beskrivelse av adferder en ønsker fra spesifikke aktører. Et enkelt eksempel er «Stat A tilbyr og gir militær støtte». Rapporten gir forslag til hvordan en kan gå frem for å kartlegge statssikkerhetsinteresser, og hvordan disse uttrykkes og illustreres i henhold til en relasjonell maktmodell.

Oversikten over essensielle statssikkerhetsinteresser beskriver staters viktigste verdier, hvilket gir opphav til navnet en verdibasert tilnærming til forsvar. Med hensyn til ovenfornevnte tre oppgaver innebærer den at skade inntreffer når fremmedstatlige påvirkningsaktiviteter har uønskede effekter på essensielle statssikkerhetsinteresser. Formålet med forsvarstiltak er å lette på denne skaden. De som får i oppgave å forsvare mot påvirkning behøver derfor en måte å vurdere sammenhenger mellom fremmedstatlige påvirkningsaktiviteter og essensielle statssikkerhetsinteresser. Rapporten tilbyr en metode kalt «sett-generering» som hjelpemiddel i denne prosessen.

Rapporten anbefaler at den verdibaserte tilnærmingen videreforedles og testes.

Contents

1 Introduction

How can states defend themselves against foreign influence? In the 2010s, a more assertive Russia has put its own spin on power in the information age. Subversive activities known from the Cold War (i.e. active measures) have been reinvented using the opportunities offered by modern technology (see for instance Abrams, 2016; Daniels, 2017). Russian influence activities on Twitter are perhaps the most well-known, and the scope and scale observed in Ukraine since the annexation of Crimea in 2014 have earned it the nickname «Firehose of Falsehood» (Paul & Matthews, 2016). However, similar activities in two electoral interventions are now also widely known (see for instance Greenberg, 2017; Haines, 2015; Jamieson, 2018). Western states' need for a well-functioning approach to defence against foreign influence is arguably greater today than it was only a decade or two ago.

Influence has of course played a role throughout history. Various forms of electoral interventions, for instance, are relatively commonplace (see Levin, 2016). But the utility of conventional military force as a tool for policy is declining, relative to that of irregular means (for more, see Diesen, 2018)[1]. Furthermore, modern societies' reliance on and use of information and communications technology (ICT) have opened new opportunities. Russia's use of social media as a tool for influence (see Chen, 2015; but also Garmazhapova, 2013) is but one example of this. China appears not only to share a view on information warfare more similar to Russia, but also a similar view on its potential utility for achieving desirable outcomes at low intensities on a spectrum of conflict (Hoffman, 2016).

Developments like the above have led to increased attention and efforts to better understand influence in the West. Influence is now widely discussed in the media, academia and at higher levels of government, and significant resources are devoted to map and describe modern (Russian) influence campaigns and analyse their aims[2]. Despite these efforts, there are arguably fundamental gaps in our knowledge, some of which have existed for quite some time. The West's de facto concepts for influence – Strategic Communication[3] (StratCom) and Information Operations[4] (InfoOps) – are lacking, and have been critiqued at length by others (see Brooks, 2009, 2011, 2012; Paul, 2011; Paul & Matthews, 2016; Tatham & MacKay, 2011; Thuv & Duistermaat, 2019). Similarly, shortcomings in Western states' understanding of defence have

[1] In his report, Diesen (2018, p. 7) defines irregular means as «ways of operating distinct from the tactics and techniques that are commonly used by conventional military forces.»
[2] The main exponent for this development is arguably the Strategic Communication Centre of Excellence established in 2014 in Riga, Latvia. Many reports on the subject is available on their webpages (www.stratcomcoe.com). Another example is Oxford University's Computational Propaganda project, or COMPROP for short (see https://comprop.oii.ox.ac.uk/).
[3] Current NATO policy defines Strategic Communication as «[t]he coordinated and appropriate use of NATO communications activities and capabilities – Public Diplomacy, Public Affairs (PA), Military Public Affairs, Information Operations (Info Ops), and Psychological Operations (PSYOPS) as appropriate – in support of Alliance policies, operations and activities, and in order to advance NATO's aims.» ((PO(2009)0141, 2009).
[4] Current NATO policy defines Information Operations as «a staff function to analyse, plan, assess and integrate Information Activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and [North Atlantic Council] approved audiences in support of Alliance mission objectives.» (NATO, 2014).

been highlighted in the past, including the tendency to focus on documenting the adversary's activities rather than what to do about it (see Chotikul, 1986).

The Norwegian Defence Research Establishment (FFI) has had a research project on influence since 2015. In that time, we have produced reports on strategic narratives (Alme, 2019b) and fake news (Alme, 2019a), influence and social media (Bergh, 2019) as well as on psychological mechanisms (Bjørnstad, 2019). In December 2015, the project was tasked to begin work on a theoretical framework for military influence operations. The task was given knowing that an entire theoretical framework was unattainable with the time and resources given, but, importantly, believing that the work itself nonetheless would lead to interesting and useful research. This report contains results from that effort, asking: How can states defend themselves against foreign influence?

The remainder of this introduction provides a brief discussion on defining influence, before we look deeper at our research question – defence – and three key tasks we argue are part of any defence against foreign influence. A key limitation in this report is that it looks only at those three tasks. We then discuss the importance of a clearly stated purpose of defence against foreign influence. A clearly expressed purpose is important as it shapes an approach to defence, and we hold the purpose is to defend state security. Finally, we provide a brief overview of our methods and the theoretical framework used to model influence in this report.

1.1 On defining influence

What is influence? We could here refer to the aforementioned definitions of StratCom or Info Ops, or even broader scope studies on phenomena like political warfare[5] (for an in-depth look at these types of ideas, see Robinson et al., 2018). Somewhat counter-intuitively, this report does not offer or adhere to any specific definition of influence. Instead, we define an approach to defence that can accommodate any type of influence activity; from funding of political parties or movements and organising demonstrations, to propaganda in its various forms both online and offline, and the manipulation of industrial control systems using cyber power.

The main target audience of this report is government practitioners tasked with defence against foreign influence. Most readers will have some grasp of what influence is; they can name relevant activities (e.g. trolls on social media), incidents (e.g. Operation Infektion[6]) or perhaps even key ideas (e.g. StratCom, coordination, information warfare, political warfare). There will still be significant variation between experts. Some may emphasize the role of information or communication whereas others may emphasize the role of peoples' minds, computer systems or

[5] Kennan (1948), for instance, defined political warfare as «the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP--the Marshall Plan), and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.»

[6] Operation INFEKTION was an early 1980s attempt by the Soviet Union to make people believe AIDS was the result of experiments in biological warfare carried out by the United States (Boghardt, 2009).

organizational processes (for an in-depth discussion on the various professional takes, see Paul, 2011; but also Brooks, 2009, 2011, 2012). Readers not in the target audience have likely read the report so far with very different types of «influence» in mind. Some may have latched on to influence as used in everyday language. Others still may have read what for instance philosophy, political science, sociology or computer science usually mean by it. The fact that other fields contain knowledge associated with the term, however, does not mean it necessarily applies or is useful in this context.

The context here is defence. Undue focus on the immediate activities and effects (typically disinformation, how it spreads, what it might do to people) arguably blinds one from the larger picture of what states and armed forces are trying to achieve in this space. It is not the disinformation itself, after all, that seems threatening; it is what it might lead to. Even if we could precisely define the list of activities or effects that constitute influence (and, implicitly, those that do not), much would remain for states to understand and defend against it. Indeed, the immediate effects of influence activities may not be of prime interest either. How far should we chase the causal chain, to describe something useful for defence? Again, it is not the activity itself, but something it leads to which might require a defence. Defining influence in terms of effects (e.g. on peoples' attitudes or opinions) leaves us wanting a further description that describes harm to states.

1.2 Three tasks for any defence against foreign influence

One place to begin explaining our approach to defence is with stating our take on what we seek to accomplish as researchers in this field. Here, we argue the main objective of this field is to enable states and armed forces to use and/or defend against influence. A concept for influence, in this view, describes how states and/or armed forces accomplish that at a level of ambition; it suggests a practical solution to the problem. As researchers in this field, we seek the tools to create and test such concepts. This report does not attempt to describe a complete concept for influence, but also does not inherit from an existing concept (StratCom and Info Ops are de facto concepts, due to their prevalence today). In line with establishing our own argument, we specify three tasks we argue belong in any concept for influence. These are:

- Define what constitutes harm.
- Assess what foreign influence harms.
- Describe the objective of defence measures.

The authors hold these to be obligatory tasks to perform in any defence against foreign influence. To have a meaningful defence, states must be able to state what they consider harmful. To say a defence is required, an assessment must conclude foreign influence is in fact causing harm to something. Finally, the above considerations are important inputs to describing an antidote. If the main objective is to enable states and armed forces to use and/or defend against influence, a concept for influence is arguably incomplete until it addresses them.

The above perspective already is very different from what is common in the field today, and the three tasks of course belong to a larger list of tasks that a more complete concept for influence should address. A number of tasks remain to discover and describe beyond the three formulated here. An example would be whether and how to integrate it into existing planning processes. To discover and describe these tasks, and then to create alternative concepts for influence that solve them differently, and finally to evaluate them against one another, is an important endeavour in this field. Such exploration may also enable improved assessments and testing of existing influence-related concepts. It is our belief that assessments would find StratCom and Info Ops to be lacking, if more of the underpinning research was conducted.

The report further reduces the scope to consider defence of liberal democratic states against foreign influence. Foreign influence clearly occurs throughout the spectrum from peace to war (theoretical discussions and empirical examples found for instance in Diesen, 2018; Hoffman, 2016; Intelligence Community Assessment, 2017). Current thinking therefore suggests such threats could manifest early and persist for some time, unbeknownst to the target. Finally, influence, and, presumably, defences against it, may take time to come into effect. It seems unreasonable to reduce the scope to war (which is also a unit of time) and the role of the armed forces (which partly follows from political goals of states engaged in war) when the governments approach to the problem is likely important to determine of the armed forces' approach. Future studies can rather explore these special cases.

Intrastate-contexts (typically internationalised intrastate conflicts, such as Afghanistan, among Western states) proved too different from the problem of interstate influence as work on the report progressed (for an interesting take on the role of narratives in intrastate conflicts, see Alme, 2019b). Discussions based on non-state actors or more authoritarian states, may turn out differently. Defence from the perspective of armed forces (e.g. to reach operational objectives in military operations) is also not considered. We elect instead to maintain focus on interstate fundamentals, which point us toward the political and strategic rather than operational and tactical levels of command. Furthermore, the use of influence, including as part of defence (e.g. how to defend against the harmful effects of disinformation using information), is also not considered.

To summarise, the report considers three tasks for defence from the perspective of a state actor engaged by another state actor. This is a significant reduction in scope from the topic of influence in general, which concerns how states and armed forces can use and/or defend against influence. It is nonetheless a wider scope than is common in this field, where the mainstays of StratCom and Info Ops usually serve as starting points.

1.3 On the purpose of defence

The purpose of defence is a key determinant of what an approach to defence against influence should look like. Having a clearly stated purpose is therefore very important. The purpose of defence shapes how success is measured. It therefore also helps determine what constitutes a valid defence measure, and how to gauge its utility.

The importance of a carefully selected purpose of defence is simple to demonstrate. If states for instance decide to combat disinformation purely on because the existence of disinformation is undesirable, any defence measure that reduces the amount of disinformation is useful. Estimates of how much disinformation there is on the Internet, for example, become interesting metrics. If states decide to protect economic interests against harm from disinformation, however, other defence measures and metrics may become interesting. Perhaps only a few specific items of disinformation in certain areas are harmful in that instance. Perhaps defence measures have more to do with economic interests than with disinformation. The point is that changing from one purpose to another likely requires a re-evaluation of the approach to defence. The purpose of defence is a key determinant of what an approach to defence looks like and having a clearly stated purpose is thus very important.

That what you seek to accomplish determines what it is meaningful to do is obvious but deserves emphasis here. Amongst other things it means that copying influence concepts from non-defence contexts should be done with care, if the objective is to mount some sort of defence of a state actor. Yet this issue has proven to be challenging in the past with respect to StratCom. StratCom was, after all, originally an idea used by businesses to brand themselves and sell commercial products to consumers. In her testimony before the U.S. Congress on the subject of StratCom, Rosa Brooks explained at length the difference between StratCom by states in support of their interests, and StratCom by private companies for the purpose of profit (Brooks, 2011).

Furthermore, disunity among multiple defence measures may indicate no common purpose in defence against foreign influence. What, for instance, is the objective of defence measures that publicly disprove adversaries' lies? The «detect and disprove»-strategy is often discussed and to some extent implemented by many governments. The purpose of one such service run by the European Union today is «to better forecast, address, and respond to pro-Kremlin disinformation.» (EUvsDisinfo, 2019). What, then, is the objective of forecasting, addressing, and responding to this subset of disinformation? How does it tie to European security, in the end? Are there better (more effective, cheaper, quicker etc.) defence measures for accomplishing the same? (for more on the origins of EUvsDisinfo, see European Council, 2015). Can a public detect-and-disprove-service have harmful side effects[7]? Do the benefits outweigh them? How good must a detect-and-disprove-service become to be effective, and does having one amount to an effective defence against foreign influence? Why? These seem to us very important questions. A clearly stated purpose is the starting point to assess all these things, and therefore also to gauge the utility of defence measures.

In sum, we hold that an approach to defence against foreign influence must have a clearly stated purpose. The purpose selected by us in the next chapter is of course a subject for debate, but the necessity of a clearly stated purpose is arguably less so.

[7] Being the arbiter of what is true and false can be very difficult, and EUvsDisinfo has issued corrections due to complaints from the Netherlands (EUvsDisinfo, 2018).

1.4 Scope, methods and theoretical framework

The general research question of this report is: How can states defend themselves against foreign influence? Chapter 2 discusses two assumptions made in this report, which leads to a more specific version of the research question: How can government practitioners defend state security against harm from foreign influence without knowing the effects of foreign influence on state security? This phrasing reflects our goal of helping government practitioners, whomever they are, to solve a practical problem. It reflects our view on what that practical problem is: defend state security against harm from foreign influence. Finally, it reflects a key conclusion from our review of the literature: estimating the effects of foreign influence on state security interests in near real-time is extremely difficult, and not something government practitioners are likely to have.

We propose a defence against foreign influence can be found in what we call a value-based approach to i) define what constitutes harm from foreign influence, ii) assess what foreign influence harms, and, iii) describe the objective of defence measures. These tasks, we argue, are obligatory in states' broader effort to erect a meaningful defence against foreign influence.

We employ a relational model of power to describe a value-based approach (see Nye, 2011 for an excellent introduction). A relational model of power can hold information on the actors and values relevant to state security and expresses them in terms of a behaviour. We here use those descriptions to define what a given state considers to be harm from foreign influence, and what the objective of defence measures is. Finally, the report must then provide some way of assessing what foreign influence harms. A method is provided for considering whether a set of foreign influence activities should be considered to have such an effect. We also seek to exemplify the implications of our work by discussing a common defence measure (strategic narratives).

A relational model of power plays a central role in our approach to a value-based defence: it is used as a theoretical framework to model our problem. The idea of using a relational model of power to understand the problem of foreign influence is inspired by Joseph S. Nye's book *The Future of Power* (2011). There, Nye uses it to explain a similar phenomenon called soft power. We have used a relational model of power since 2016, and it remains in our view a powerful tool for structuring this problem[8]. There may well be other ways of structuring this problem that leads to very different ideas for defence.

In this report, the term «reactive defence measure» refers to the defence measures government practitioners decide to enact based on observed foreign influence activities. The term «proactive defence measure» refers to defence measures government practitioners decide to enact based on other considerations than observed foreign influence activities. The national narrative and state

[8] For a time, we did try and describe some of the power resources and power behaviours that might belong in such a model when applied to the problem of influence, but we were unable to produce good lists. We suspect the reason for this is that no predefined set of activities in and of themselves constitute influence. We have therefore made sure to discuss that point in our report as well and used a more rudimentary model of power because of it.

security narrative described in chapter 5.2 are examples of what is here considered proactive defence measures.

1.5 Outline of the report

This introductory chapter offered a brief introduction to why influence in general, and especially a defence against foreign influence, is an important topic today and relevant for a research institute like FFI. It also introduced the necessary background information to define and further specify our research question, including the scope and main assumptions of this report. Chapter 2 offers a broad overview of our value-based approach, including a more detailed discussion of the two main assumptions we have made. Chapter 3 details the use of a relational model of power to represent essential state security interests, while chapter 4 shows how to use that information as a basis for defence. Chapter 5 showcases some of the implications of a value-based approach to defence through a discussion of a defence measure that is often proposed: strategic narratives. Finally, chapter 6 offers a summary and concluding remarks.

2 An overview of a value-based approach

Section 1.2 outlined three tasks for any defence against foreign influence: i) define what constitutes harm from foreign influence, ii) assess what foreign influence harms, and, iii) describe the objective of defence measures. These tasks can be solved in several ways, but government practitioners, solve them under a specific set of circumstances. There may not be time for academic rigour, for instance. This chapter explains two key assumptions the authors hold as reasonable to ensure practical utility for states and government practitioners. It further provides a broad outline of the value-based approach, and an introduction describing the effects of foreign influence in a manner that adheres to the two assumptions.

2.1 Two key assumptions

The value-based approach rests on two key assumptions that are important to make explicit:

1. It assumes that the purpose of defence is to protect state security.

2. Practitioners are unlikely to get accurate measurements of whether foreign influence is harmful, and how harmful it is, by the time they must formulate defence measures.

The first assumption stems from the discussion in section 1.3 on the importance of a clearly stated purpose. The purpose of defence against foreign influence is to protect state security because that is what matters most to states. This assumption – this purpose – means that a

successful defence is a defence that successfully defends state security against harm from foreign influence. To say that foreign influence is harmful, and requires something be done about it, thus requires an argument be made that connects activities to harmful effects on state security. Defence measures are required when foreign influence harms state security, and their objective is to alleviate that harm. Any proposed defence measure must therefore be supported by an argument, to show how it reasonably protects against that harm. This assumption, in short, requires all tasks – defining harm, assessing harm, and describing defence measures – be solved with state security as their purpose.

Defining state security will obviously be a central challenge. Another challenge lies in setting reasonable requirements for the arguments practitioners must put forth to say that 1) foreign influence is harmful, 2) defence measures are required, and 3) a specific defence measure protects state security from that harm. This report uses a simple relational model of power to set the basic rules for how state security is defined and expressed and uses that view of the world to anchor the discussions practitioners must have.

The second assumption, that practitioners are unlikely to get accurate measurements of whether foreign influence is harmful, and how harmful it is, by the time they must formulate defence measures, helps ensure that the approach adheres to the reality faced by practitioners. Practitioners will not be aware of all harmful activities, and even if they were, they are unlikely to have detailed and reliable measurements of their effects on state security. From our review of the literature, we do not believe researchers can currently provide a comprehensive explanation of the causal chain between the adversary's activities and effects that harm state security, much less do so at the speeds required for a real-time picture. Knowledge in this area is certainly useful, but as of now limited to certain segments of that longer causal chain.[9] Government practitioners today are therefore unlikely to have high quality information in these areas when they must consider a response, and an approach to defence of practical use today should not assume that they would. The effects of foreign influence activities on state security are therefore, as far as this report is concerned, unknown[10].

2.2 Outline of approach

The above assumptions allow for further specification of the research question. Since the purpose of defence is to protect state security, and arguments that connect foreign influence activities to harmful effects on state security are required to derive defence measures, it would

[9] To give an example, take Allcott and Genzkows (2017) paper «Social Media and Fake News in the 2016 Election». This article was published in the spring of 2017 and thus only a few months after the 2016 U.S. presidential elections. The article is published quickly from a researcher's perspective, but after the fact in terms of deciding whether fake news threatened the U.S. election and what could and should be done about it. The article presents interesting knowledge on several interesting aspects of how people came into contact with and perceived fake news. But it is also not meant to describe the impact on the behaviour of U.S. citizens at the voting booth or in other ways that might affect U.S. state security interests. Fake news is of course but one of several activities that in theory (and perhaps in combination) alter that sort of behaviour. It thus becomes one piece of information in the much larger puzzle that government practitioners must contend with.

[10] Decent analyses of the Russian influence campaign during the 2016 US presidential elections exist, but have taken years to produce (the first in-depth analysis of the role of social media is arguably Jamieson, 2018).

be important to discuss how to provide practitioners with reliable measurements of effect. The second key assumption, however, says practitioners are unlikely to have such measurements in time. The research question is therefore: How can government practitioners defend state security against harm from foreign influence without knowing the effects of foreign influence on state security?

To address this question, we propose to look inwards, rather than outwards, for an approach to defence. Instead of documenting activities and their effects, we look at how states can get to know themselves and their interests well enough to protect them. This effort to get to know themselves leads to an overview of what a given state regards as important to defend. Defence revolves around this overview; it helps direct defence measures towards something worth defending. States can thus design purposeful defence measures without knowing the exact nature or impact of the adversary's activities.

The overview serves both proactive and reactive defence. Proactive measures find their purpose in the interests – or what we here term «state security essentials», or simply «essentials» – described in this overview. Reactive measures, however, is more difficult. We recognize that practitioners will only have a window into what the adversary is (or might be) doing (i.e. some level of detection), and some knowledge of his intent. How do we understand these activities well enough for defence, when their effects are unknown? We can hypothesize the effects of an activity, but our assumptions mean the hypotheses will be untested at the time practitioners form a response. We propose that plausible arguments connecting alleged influence activities to harmful effects on the interests described be considered as sufficient to legitimize defence measures. What is considered plausible is of course a subject for discussion. In this report, the overview of state security essentials helps ensure that arguments relate influence activities to interests that are important to defend. Accepting that proposition, one path to reactive defence lies in a structured process for generating such arguments. The most important and most plausible arguments must be found, preferably in the matter of hours or days. Arguments need not be proven true, as long as the most important arguments are among those generated and defended against. Section 4.3 further details this process, called «set generation». What can and should qualify as a plausible argument, however, should be the subject for further study.

2.3 Introduction to representing effects

The purpose of defence is here to protect state security, which means a rationale for defence lies in establishing a link between influence activities on the one hand, and state security interests on the other. In our experience, descriptions of effects commonly fall short of establishing that link, describing instead the activity (e.g. the spread of disinformation on some medium) and perhaps possible effects on people (e.g. how people confuse facts with fiction). Such knowledge is obviously useful, but this report emphasizes the importance of continuing the argument until it concludes with an effect on state security. If practitioners are unable to make that argument, then it is hard to see why a defence would be necessary.

Furthermore, if state security requires a defence against foreign influence, we should also be able to express part of the harm from foreign influence in the vernacular of international relations. The threat from foreign influence between two or more states can be expressed as a form of power; states use influence to achieve preferable outcomes in international relations. It is therefore important to be able to express the harm from foreign influence, as well as the utility of proactive and reactive defence measures, in those same terms. Put differently, it would be odd to argue that a defence from foreign influence is required, and present a set of defence measures, yet not explain how it ties to international relations.

A relational model of power helps represent effects in a simple yet structured manner. As will become clear, it helps structure discussions on the harmful effects of foreign influence as well as to tie them to state security. Here, the report borrows from Joseph S. Nye's discussion on power in his book *the Future of Power.* Power is defined as «the ability to alter others' behaviour to produce preferred outcomes» (Nye, 2011, p. 10). To exert power, an actor uses power resources in accordance with a conversion strategy to achieve power behaviours. To consider foreign influence harmful and thus requiring a defence, this approach to defence requires an argument that stretches from the adversary's use of power resources (i.e. influence activities) on the one hand, to the harmful power behaviour it causes in another. Those behaviours must tie to state security (chapter 3 discusses how to do that).

In figure 2.1, State A exerts power over State B by using power resources Activity [1 … N] according to a conversion strategy in its power relation with B (arrow). Introducing new actors, helps describe contexts that are more complex.

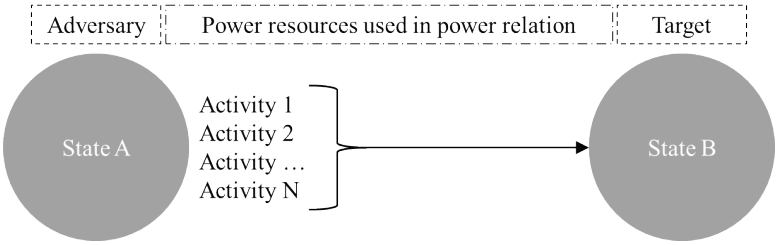


Figure 2.1 Example illustration of a relational model of power.

The above model is used because it is both simple and captures some important aspects. The fact that the model does not draw us towards any specific type of power resource or power behaviour is a strength. First, any power resource can be used for influence; there is no pre-defined set of activities which in and of themselves constitute influence (see Thuv & Duistermaat, 2019). You can consider the effects from Activity 1 alone, or effects from larger sets of activities[11]. Second, the same is true with respect to power behaviours; there is no pre-

[11] This model supports analyses of any subset of all activities, such as disinformation on Twitter or financial support of political parties or candidates but makes no claim as to how activities should be subdivided. Studies of foreign influence activities invariably study a subset (e.g. trolls on Twitter) of the larger whole, but the consequences of that reduction in scope on an analysis of harmful effects on state security are unknown. More research is required to determine how to subdivide activities for analyses of harmful effects on state security, and we would rather err on the side of caution by using an indeterminate model.

defined set of power behaviours belonging to influence. Third, and importantly, the key distinguishing features of influence lie in the conversion strategy, in its design, and what the organization supporting that process looks like to make use of it in international relations and armed conflict.

The relational model of power will form the basis for how we reason about harmful effects, as well as how we illustrate state security interests. This section only provides a simple illustration based on the power relation between two states — State A and State B — but there is clearly more to represent. We hold that the model should reflect state security essentials, and therefore move on to discuss how practitioners can create the overview.

3 Mapping state security essentials

What are the essentials of state security? What would, if harmed by foreign influence, be the most important to defend? Ultimately, the task of mapping state security essentials yields unique results for a given state, as every state is different. This section provides suggestions based on interstate and intrastate aspects of state security that are likely common to most liberal democracies. Deciding where to draw the boundary around state security is not simple; the essential state security interests must be included, but the longer the list the more expansive the defence effort. This suggests government practitioners should take care to ensure the most important items are included in the overview, but also that the overview is manageable and proportionate to the problem.

3.1 Interstate essentials

International relations are clearly part of how one understands foreign influence. Figure 2.1 showed a bilateral relationship where State A sought to influence State B, but contexts that are more complicated are easily accommodated using the same model and type of illustration. Figure 3.1 shows a context between multiple state actors, State A, B, and C. The lines between them signify power relations, and to integrate international relations into the context we define state security interests in each relation. A set of simple fictitious interests and events will help illustrate how this works.

Consider State A to be the aggressor and State C to be its target. State A wants to coerce concessions from State C through a low-intensity conflict. State C relies on State B for support in case of conflict with A, which means it is an important player in any conflict with State A.

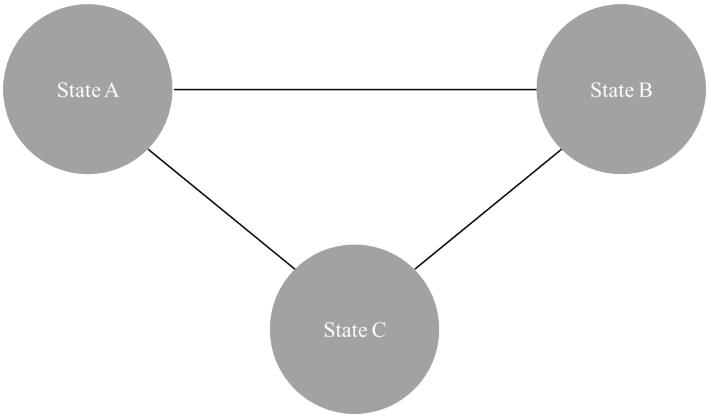


Figure 3.1 International relations scenario with multiple state actors.

Since this approach is designed for defence, we here take on the point of view of State C. What sort of effects from foreign influence is cause for worry to State C? To find out, State C defines its key state security interests in these relations, and thus gets an overview of what matters most (its state security essentials). It knows the desirable behaviour from State B is support in the event of a crisis or conflict, and the desirable behaviour from State A is that it either does not seek conflict or ceases its hostilities. These are of course but some of several possible interests that could be defined in these relations. The complete set of interests is what we mean by interstate security essentials, or simply interstate essentials.

Because State C depends on State B, there is another power relation to consider as well; that between State A and B. State C should consider State A's interests in this relation, which could for instance be to reduce the likelihood of State B offering support to State C. Whether State A intends it or not, their influence activities are a potential threat to State C's interests in relation to State B. State C should therefore consider the possibility that the threat from foreign influence looks more like that of figure 3.2.

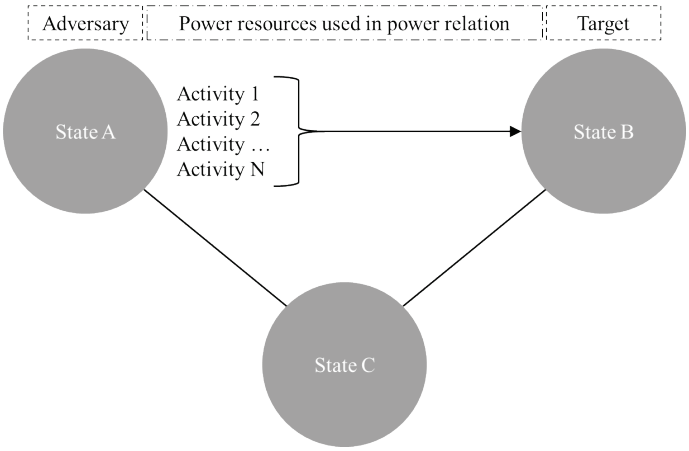


Figure 3.2 Fictitious example of foreign influence against key ally.

In figure 3.2, State A's activities reduce the likelihood of State B coming to State C's aid. In this report, this is harm to state security interests and therefore something to defend against. Even if State A does not intend to produce this effect, it is produced through his activities and should therefore be defended against. This is one of the ways in which a model like this is superior to one rooted solely in the adversary's intent or objectives. Importantly, the figure shows that there are two relations in which to mount a defence of this interest. First, State C can attempt to disrupt the activities of State A in relation to State B. Any power resource can be used to accomplish this, and the exact nature of such an effort will depend on the type of activity observed to begin with. It could include things varying from traditional counter-intelligence work to disrupting networks of bots on Twitter, and much more. Second, State C can seek to improve the likelihood of support from State B through its relation with State B. Any power resource can be used in this effort as well, including normal diplomacy. Third, it can gauge the situation and decide the current likelihood of support from State B is acceptable, and that the negative effects of State A's activities are negligible; it can choose to do nothing.

The above way of reasoning about the harmful effects of foreign influence on state security interests in international relations allows us to think more clearly about the threat. Many of Western states' current suggestions for defence measures, for instance, focus on the activities themselves. The above example shows that multiple relations can be impacted by the same activities and require a defence, and that other avenues are available for defence. This approach to defence captures this arguably important side to the threat from foreign influence. For instance, alliance members' interpretation of foreign influence as a potential threat to the internal stability of NATO can be represented much like the above figures, by replacing State B with NATO. The internal stability of NATO likely affects the behaviour that alliance members depend on from NATO.

The discussion so far has depicted a situation in which State C reacts to State A's activities. There is, however, nothing stopping State C from working proactively to protect its interests in relation to State B. The interests specified in these relations therefore also form the basis for proactive measures to defend against the harmful effects of foreign influence. Indeed, given the difficulties with detecting the adversary's activities to begin with, the overview described here not only makes us aware of the potential threat that stems from State A's influence over State B, but can help us direct our attention to better detect it. In this way, it is also a tool to help focus our detection efforts towards areas of high importance to state security.

This section introduced the core idea behind our value-based approach to defence. In practice, figures like those presented here should contain well-defined behaviours required for state security in each power relation. Concrete descriptions of interstate essentials require application of the model to a specific state, and to a set of scenarios. Application to a specific state, however, is beyond the scope of this report.

The above representation is still incomplete, even if properly detailed for a specific state. All state actors in the above figures also have intrastate essentials to defend. If, for instance, the activities in the fictitious example in figure 3.2 target the population of State B, a plausible argument is required to connect that influence to pressure on the government of State B, which,

in turn, reduces the likelihood of B having the behaviour C desires. The argument would be different if State A targeted key decision makers in State B, because the causal mechanism by which State B's behaviour is altered changes from one involving its population to one involving its key decision makers. Moreover, State A can of course target State C directly, and not through an intermediary as discussed here (although that, too, might backfire on interests in relation to State B). An overview based on interstate essentials helps structure this rather complicated picture but is clearly an incomplete representation of the problem of foreign influence. We therefore turn to intrastate essentials and return to a more complete overview in section 3.3.

3.2 Intrastate essentials

The discussion in section 3.1 concerned interstate essentials, and therefore revolved around state actors. The behaviour of state actors is of main interest here, but actors other than states of course also shape state behaviour. Indeed, one of the main reasons Western states consider foreign influence a problem is that it (possibly) does something to the citizens, which in turn (somehow) harms state security. This section represents this sort of problem using power relations, just like the problems discussed in section 3.1, but distinguishes them as intrastate essentials instead.

What are the essential intrastate state security interests of a liberal democracy? What would warrant defensive measures, if harmed by foreign influence? The report identifies intrastate essentials much like interstate essentials: by looking inwards at what matters to a given state. There is, for instance, no need for a liberal democracy to experience an electoral intervention to determine that nation-wide elections are important. Indeed, all states that hold elections want them to go as planned (even authoritarian ones). This section shows how to create an overview of intrastate essentials. First, however, a discussion of who the relevant actors are, and how to illustrate intrastate essentials, is in order.

3.2.1 Illustration and suggested actors

Figure 3.3 shows State A targeting State B through its population, meaning there are now two power relations involved; one between State A and State B's population, and one between State B's population and its State B's government and institutions as an entity. To understand how State A's influence on State B's population might become harmful to State B's security, State B must further explore the power relation with its population. If, for instance, State B is experiencing dangerously low levels of political trust, and State A is exacerbating that problem, State B might consider defence measures that rebuilds public trust (a key point, of course, is that it should rebuild it even if State A is not the cause). Alternately, if State B's population is pressuring foreign policy in a direction that harms state security interests, such as reducing the likelihood of allied support in the event of a conflict, then State B should consider options that increase the likelihood of allied support. Chapter 4 will further discuss this type of reasoning.

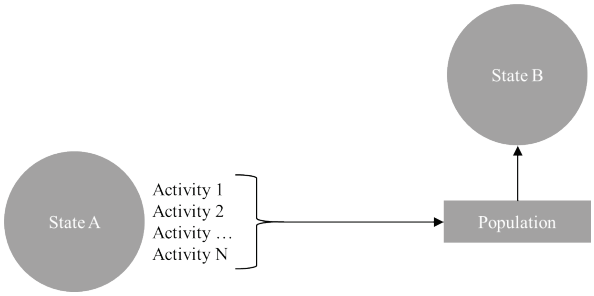


Figure 3.3 How foreign influence targeting the population may be a threat to state security.

Who are the most important internal actors? This depends in part on the state in question and its history. It may be fruitful to subdivide the population, for instance if there is a past and/or present separatist movement. There may likewise be reasons to represent the government in subgroups, such as according to the branches of government, to explore influence that may threaten checks and balances between them. Numerous areas, like policies, doctrines, norms, traditions, and principles, can help determine a useful set of actors.

In our model, all actors are represented with power relations between them, and the number of relations to consider grows quickly as the number of actors increases. For the sake of argument, this report considers a basic set of four intrastate actors: the government, the armed forces, the population, and the press. Application of the value-based approach to a specific state actor would likely yield a different, larger set of actors. Figure 3.4 adds these internal actors as square boxes. For the sake of simplicity, the circle for «state» is included in this intrastate figure as well. Keep in mind that it essentially refers to the government, and that analyses may find it useful to subdivide it (e.g. into branches of government). Here, this yields six power relations in which to describe state security interests.

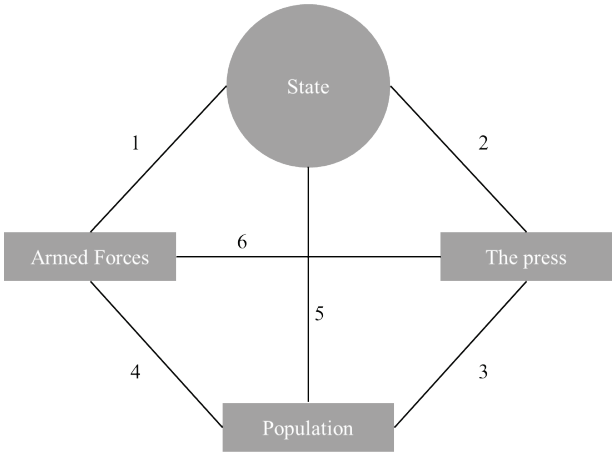


Figure 3.4 Actors for intrastate security essentials.

Having identified some plausible actors to consider interstate essentials for, we move on to discuss where and how practitioners might begin enriching the overview with security essentials.

3.2.2 Suggested starting point

What are the state security essentials of a liberal democracy? The answer depends in part on the state in question. One source of information is what academia considers signs of a healthy modern liberal democracy. This literature provides such things as general pre-requisites based in political theory (e.g. a free press, free and fair elections, democratic institutions, a public sphere providing room for public debate) (see for instance Dahl, 2005; Habermas, 1993; McNair, 2009; Sodaro, 2008, pp. 171–177; Street, 2011), but also knowledge and experience in more detail (e.g. sources of instability) as well as in measuring their status. The Center for Systemic Peace (CSP), the Uppsala Conflict Data Program (UCDP) and the Peace Research Institute Oslo (PRIO) are examples of institutions that maintain datasets on these types of factors. The sources will help create an overview of interstate essentials, but states also face more unique challenges and view security differently from one another. Another, and complementary, source of information is what states themselves consider essential. Official documents, such as defence and foreign policy documents, contain statements that can help define what state security is to a specific state.

Government practitioners must create and maintain the list, and, like interstate essentials, to a certain extent tailor it. This section will only demonstrate how to begin that process, and how to increase the level of detail until it describes behaviours in power relations. The overview could of course grow very long. A guiding principle may therefore be to ensure it contains what matters most, and little else. The following three topics should serve as useful starting points for liberal democracies (see §1-5 in Lov om nasjonal sikkerhet (sikkerhetsloven), 2018):

- Territorial integrity.
- Political sovereignty.
- Democratic processes.

From this basic list, work continues by further detailing each topic. If there are sub-topics, as there will be with respect to democratic processes, for instance, these may require elaboration as well. The objective is to arrive at a level of detail that allows for expressing behaviours in power relations between the identified actors. Describing desirable behaviours for each power relation, for all identified interests, completes the mapping process. Below is an example question for one interest in one power relation:

Consider the power relation between the population and the armed forces (power relation between actors). Do the armed forces depend on the population's behaviour to ensure territorial integrity (state security essential relevance in relation)? If so, describe this behaviour, and place the description in the power relation between the armed forces and the population. Consider multiple scenarios, and ensure that the text captures any differences between them. What impacts the likelihood of observing those behaviours when they are needed? What is considered harmful behaviour, and what is not? Why?

The process of identifying and detailing state security interests and actors, and discussing each interest for each power relation, yields a more comprehensive understanding of what harm from foreign influence could look like. It provides practitioners with a reproducible way of distinguishing between what is and is not harmful, and thus solves one of the main tasks explored here; defining what constitutes harm.

Practitioners can look for further information in law and policy documents. Norwegian law, for instance, contains a definition of national security (see §1-5 in Lov om nasjonal sikkerhet (sikkerhetsloven), 2018). It refers mainly to Norwegian sovereignty, territorial integrity, and democratic form of government. States' core interests are typically territorial integrity and political sovereignty. The idea of sovereignty is constantly evolving, and the importance of territory as a source of wealth as well (see Biersteker, 2002). What matters here is to capture their essence, along, perhaps, with any given states' specific views. Norwegian law offers more detail, such as economic stability, which is helpful in mapping Norwegian state security interests.

Major policy documents can offer similar definitions, such as: *«National security means preserving the existence, sovereignty, sovereign rights and integrity of the country. National security may be challenged through armed attack, political and military pressure, and serious strikes against Norwegian interests by state or non-state actors. Threats to national security may legitimise the use of all military and other resources»* (Norwegian Ministry of Defence, 2015, p. 7). Regardless of what sources are used, it is most important to arrive at an assessment that is government approved. It will form the backbone of the way practitioners argue about the harmful effects of foreign influence and the objective of defence measures.

Territorial integrity, political sovereignty and democratic processes are high-level descriptions, and likely to yield a host of sub-topics to explore further. Democratic processes, for instance, consists of many sub-topics, such as popular sovereignty; free, fair, open, and regularly repeated elections; a free press that holds the government accountable and citizenry sufficiently informed; freedom of speech; freedom of association; free political opposition; the rule of law; and more. To complete mapping intrastate security essentials, each sub-topic must be described

and then discussed for every possible power relation. The simple beginnings of the three tasks summarised in bullet points at the beginning of this report may be more than enough for an initial pass at using this approach. To illustrate, the report will look closer at one of the above subjects: a free press.

3.2.3 A free press

The terms «journalism» and the «free press» refer to a profession, to a form of discourse and genre, to a democratic and idealistic mission, and to an institution. The common denominator is the core reference to the search for and public distribution of information that is true and relevant to the citizens of a democracy (Eide, 2011, p. 10). The news profession is supposed to constitute a credible source for public knowledge dedicated to finding and spreading information for the common good (Jones & Baym, 2010, p. 280). Journalism is, according to the ideal, supposed to contribute to essential conditions for democracy – in several ways. For one, journalists are supposed to provide citizens with information they need to be free and autonomous; to understand the reality around them; and to be able to act and partake in democracy (Eide, 2011, p. 12). Secondly, journalists are to provide the government the information it needs to make decisions in the common interest and sensitive to the will of the people (Sjøvaag, 2018, p. 2). Thirdly, the media is supposed to create an arena for public discourse and debate. Lastly, the press is supposed to act as a watchdog on behalf of the people by way of informing citizens of what the government and other powerful actors are doing in their name, scrutinize the powerful and reveal and inform about any potential breaches with essential principles of liberal democracy, such as sovereignty, balance of power, and the rule of law (Sjøvaag, 2018, pp. 4–5).

What are the conditions for such a free press to function according to the described ideal? One condition is that there must be an established press profession in the state in question. This means journalists, editors, donors – public or private – are standard-bearers for the profession. They provide federations, ethical and professional rules to which the media companies can ascribe and adhere, and a form of professional response to breaches with such guidelines. This enables the press to go about their work in an orderly manner, but it also contributes to the overall credibility of the press as a democratic institution.

Another condition is that the press commits themselves to such rules, which are self-imposed and nonbinding (see McQuail, 2003; Sjøvaag, 2018). Sjøvaag (2018, p. 15) further argues that «[d]emocracy as a form of government is wholly reliant on private media to fulfil social contract obligations. Beyond public service broadcasting and other state-sponsored information infrastructures, freedom of expression and freedom of publication—as liberal principles—are premised on private enterprise, as governments cannot legitimately be held responsible for providing the only available scrutiny of their own affairs». Conversely, citizens will not be able to scrutinize – let alone stay informed of – these same affairs without the help of the press.

The press is dependent on the state in terms of support (interviews, donations, trust in the information, source criticism) and non-interference with the freedom, integrity and autonomy of the press – which in effect supports and makes possible a free press.

The press is dependent on a public that is willing to contribute to reporting in the form of interviews and supplying information, as well as purchasing publications. But in a more profound sense, the institution of journalism is dependent on a public that dedicates itself to finding true and relevant information: «the democratic ideal depends on an active and educated citizenry (Barger & Barney, 2004, p. 195)». As such, «the press needs a public willing to take the time to inform itself, that will engage and talk to journalists and one another, that is willing to invest resources for quality of information» (C. Marvin & Meyer, 2005, p. 409). Herein lies a premise that citizens not only actively seek information, but also critically evaluate information and sources.

The above are but examples of knowledge on a free press that will help practitioners identify important topics and behaviours to describe in the various intrastate power relations. To give a few examples of essentials formulated in preferred behaviours, based in the above:

1. In the power relation between the population and the press, it is important to note that the population in large takes the time to inform itself, engage and talk to journalists, to one another, and invest in quality information. Consequently, if foreign influence is understood to threaten these behaviours, or they are, for any other reason, not at satisfactory levels, a liberal democracy should consider measures to foster that sort of behaviour.
2. In the power relation between the state and the press, the state depends on the press to impose the contractual bonds that make it a free press on itself. If this is not occurring, or not occurring at satisfactory levels, states can consider measures to foster that sort of behaviour.

These two bullets illustrate how digging deeper into why certain things are important to state security will yield an understanding of what could be considered harm from foreign influence and point towards purposeful defence measures. As the overview of state security essentials develops, ever deeper analyses will be required. Various disciplines will offer relevant methods and knowledge.

3.3 Basic overview of state security essentials

Sections 3.1 and 3.2 show how government practitioners can create an overview of state security essentials and express them (preferably as behaviours) in power relations between actors. This yields an overview of values with respect to actors, expressed in a way that lends itself to thinking clearly about the harmful effects of foreign influence and about defence. The number of interests and actors will vary from state to state but is also, as expressed earlier, a matter of how governments themselves define security.

Figure 3.5 shows State A targeting the population of State B using Activities [1 … N]. State B has defined security interests for the power relations between the population and the armed forces, press, and government respectively (numbered 4, 3 and 5 respectively). This is how our value-based approach represents the (common) argument that foreign influence does something to the population, which, in turn, harms state security.

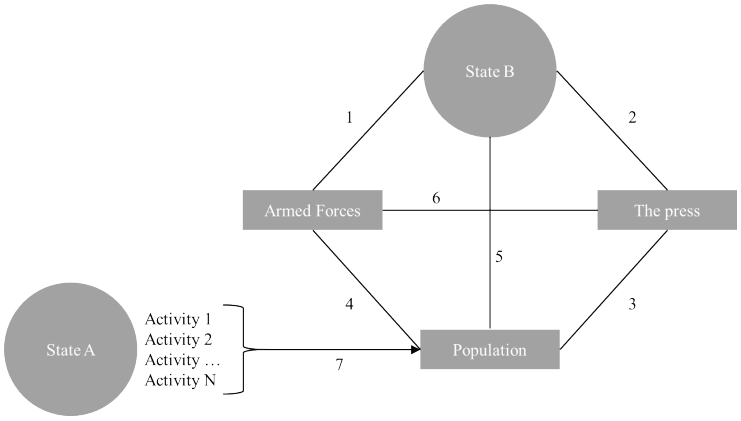


Figure 3.5 Example disinformation campaign.

Figure 3.5 can represent a number of arguments in a meaningful and structured manner. Figure 3.2, in section 3.1 on interstate interests, showed an example of foreign influence subverting the likelihood of allied support. Figure 3.6 shows the same argument, but with the added detail offered by intrastate essentials. It shows State A influencing the population of State B, to reduce the likelihood of its government offering support for State C in the event of a conflict between State A and C. One might also say the argument follows a vector of power relations, which in this case is [a1, b5, c7], and that relevant defence measures could protect interests along it to protect the state security essentials defined in [c7].

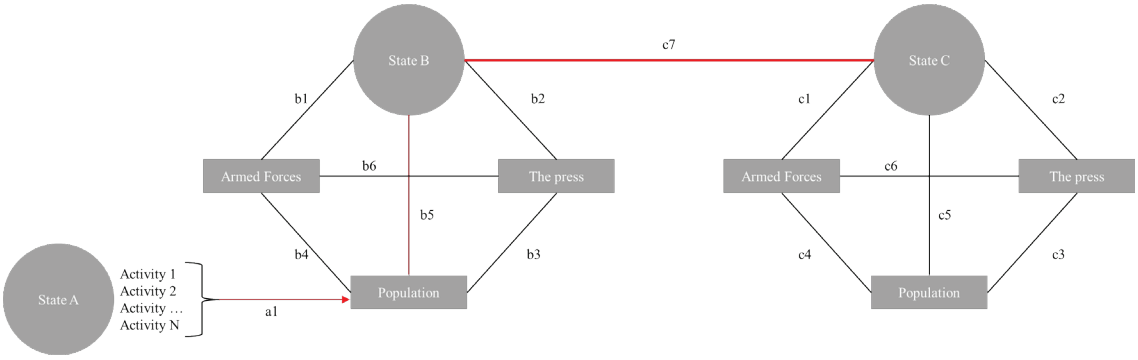


Figure 3.6 State A subverting allied support from State C to State B.

Importantly, all of the information required for State C to describe its interests in power relations [c1 … c7], and how c7 might depend on power relations [b1 … b6], is available prior to any influence activities conducted by State A. State C can therefore use that overview of state security essentials for both proactive and reactive defence, which is the subject of chapter 4. Moreover, it can do so even with limited knowledge of what State A is doing and achieving.

The above understanding of state security serves as a framework into which existing knowledge can be placed. Existing knowledge sheds light on small areas of it: specific interests as they are

described in specific power relations. Knowledge of how fake news on social media impacts voting during nation-wide elections (e.g. Jamieson, 2018), for instance, is likely relevant to the relation between the population and the state, and the way both of them are tied to nation-wide elections. Moreover, such an incident will likely impact interests in relations to other states, for instance if the perception is that a government is illegitimate.

Importantly, knowledge from many fields, such as media and communications, computer science, sociology or psychology, is required for an enriched understanding of state security essentials and their status. That understanding can in turn help evaluate the utility of defence measures. The model described here points out key aspects of any argument regarding the harm from foreign influence and the utility of defence measures.

4 Using the value-based approach to defence

Previous chapters provided tools to represent the effects of foreign influence (power relations) and define what matters most to states (mapping security essentials). These tools provide practitioners with the basic building blocks required to describe how foreign influence is harmful to state security (see sections 1.3 and chapter 2). This section describes how to use this knowledge to derive a purposeful defence of state security. It considers both proactive and reactive defence throughout any spectrum of conflict, and a good place to start this discussion is with the problem of distinguishing peace from conflict.

4.1 Defence and the interim between conflict initiation and discovery

It is common to distinguish between a spectrum of conflict, and to treat the transitions from one to another as a significant event and point in time (e.g. a crisis begins with the transition from something into the crisis). Identifying these transitions can be difficult, however, and the terms used can vary from case to case and between disciplines. Then come the added difficulties with distinguishing between peace and conflict when the means used are low-intensity, non-conventional, or irregular (for more, see Hoffman, 2016). Many foreign influence activities can and do fit into such contexts. For this reason, we believe it is necessary to contend with the possibility of an interim: that foreign influence activities go on for some time without being detected by the target.

To explore the possibility of an interim we conduct a simple thought experiment, using the relationship between our two states, State A and State B, once more. Let's assume that after a period of peace between the two, State A decides to initiate unconventional warfare against State B. According to Hoffman (2016, p. 30), such warfare «can occur concurrently with other methods in both peace and war.» Let's further assume that if we analysed some of State A's

activities as influence activities, we would find harmful effects on the state security essentials of State B. State B, however, has not yet discovered the full range of State A's activities – or not understood their influence potential. If State B had sufficient information and understanding, they would enact defence measures of several state security essentials. They do not, however, in our thought experiment here, and do nothing. There now exists an interim between State A's initiation of what we for our purposes here label conflict – their unconventional warfare – and State B's discovery of that same conflict. Indeed, there is also in principle the possibility that State A achieves its aims prior to State B discovering the unconventional war – i.e. that conflict discovery is too late, if it occurs at all.

Figure 4.1 illustrates the above scenario, using a greyed-out area to denote an interim prior to State B's conflict discovery. Please note that the terms peace and conflict here are simple descriptors to help us separate two periods of time with respect to an adversary's initiation of influence activities and the target's discovery of them. At what point, if any, these activities establish a broader security context like that of an armed conflict, a so-called hybrid war, a militarised dispute, or some other form of conflict, is another matter entirely.

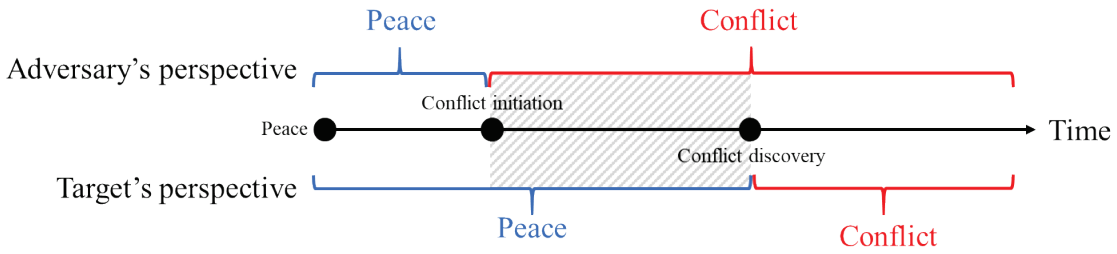


Figure 4.1 An interim between State A's initiation of an unconventional war and State B's discovery of it, and its consequences for how the two parties perceive the situation across time.

This report assumes that the effects of foreign influence are unknown (see section 2.1) and does not claim to know how harmful influence activities in an interim can be. It rather notes that this is a theoretical possibility, and that states seeking defence during an interim must look to proactive defence measures. If the target state maps out its state security interests, and engages in proactive defence, then the adversary's successes in this interim might be limited or curtailed. This seems an important lesson for defence against influence in low intensity contexts.

4.2 Proactive defence

Proactive defence here means to secure the interests as defined in the overview of state security essentials, using any power resource. Proactive defence rests mainly on the overview of state security interests created by applying mapping as described in chapter 3 to a specific state actor. Figure 4.2 shows a simple mock-up used to explain how. An actual overview would likely contain more actors, specify a scenario (e.g. peacetime, a specific conflict scenario), and fully detailed as per sections 3.1 and 3.2.

As in previous figures, State C depends on its ally, State B, for defence. State B is therefore included as an actor and power relation [c7] describes State C's dependency on B. It describes it in detail in accordance to sections 3.1 and 3.2, and therefore recognizes the various contexts in which support from State B is required. State C's overview of state security essentials includes such things as various forms of support, the timing of support, or analyses of whether it will be easy or challenging to attain etc.

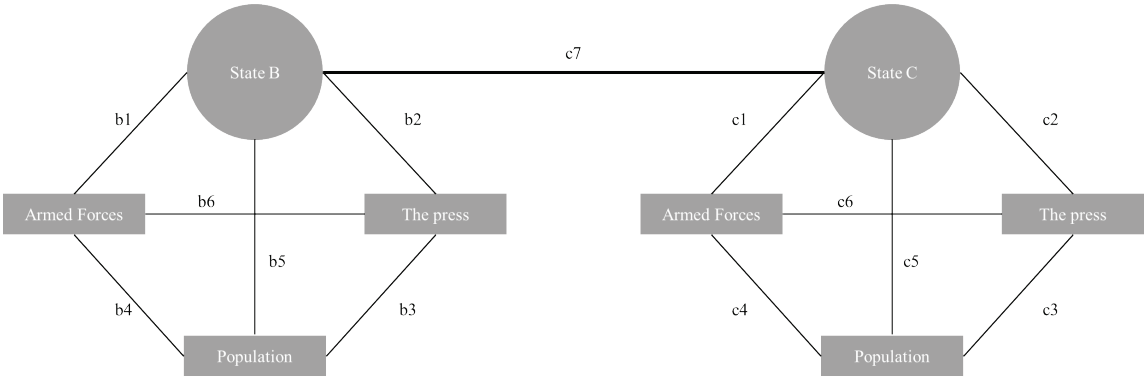


Figure 4.2 Example overview with power relations between interstate and intrastate actors. Essential interests would be defined in each of them.

Figure 4.2 is void of any foreign influence activities; there is no information on State A's (possible) activities. Proactive defence here means to secure the interests as defined in the overview of state security essentials, using any power resource. In principle, State C can seek to further all state security essentials. It may be advisable to use the information collected in the overview to establish indicators of the status of each essential. In the short run, measuring the status will help states focus their proactive efforts. If one of State C's problems is low levels of political trust, as an example, and political trust is a state security essential, then State C should seek to remedy that situation. If political trust in State C returns to acceptable levels, efforts can shift elsewhere. There is no reason to fix what is not broken.

We can translate this into a more general point: determining and measuring the adversary's activities' role in the negative development of a state security essential is secondary, and not necessarily critical for defence. Of main interest for defence is to determine whether a state security essential is trending to unacceptable levels, and to figure out how to reverse the decline. The above logic will help practitioners to pinpoint strengths and weaknesses, as well as to describe what defence measures should seek to accomplish (e.g. return political trust to a certain level). It does not help derive the actual defence measures, and using influence is but one of several possible options.

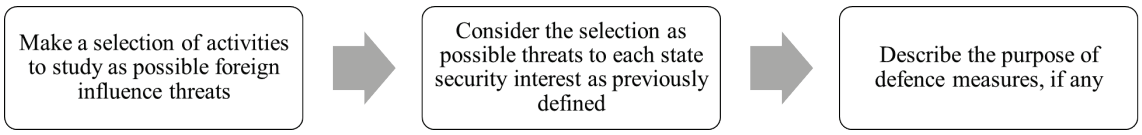
4.3 Reactive defence – 3 steps of set generation

The discussion of how to represent international relations in the overview of state security essentials has revolved around an example where State C had reason to enact defence measures against the foreign influence activities of State A, to preserve or improve the likelihood of

military support from State B. That example showed the basic logic of reactive defence in this report, where harm is expressed as harm to state security interests, and defence measures seek to avoid and reverse that harm. This section describes a method for assessing the possible harmful effects of foreign influence, and deriving the purpose of reactive measures, based on the overview of state security essentials. The report terms this method «set generation».

Set generation is a «quick and dirty» way of assessing the harmful effects from foreign influence. It sacrifices knowledge about the actual effects of foreign influence on state security and substitutes it with a set of possible effects. Whatever knowledge exists can of course be used, but the process itself does not rely on it. The objective is to ensure that the set contains the subset of arguments that are both correct and most harmful to state security. The entire set forms the basis for reactive defence, thus allowing for defence at greater speed than one driven by precise measurements of effect. The overview forms the basis for expressing plausible arguments on the harm from foreign influence, thus giving defence measures a clearer state security purpose.

The core idea of set generation is to interpret the adversary's influence activities as potential threats to all interests on the overview of state security essentials. Practitioners take a selection of foreign influence activities, and then consider that selection against interests as defined on the overview. Iterating through the entire overview produces an assessment of harm for that selection of possibly harmful activities, up against what a given state considers most important. Because the assessment ties to the map, it will also point practitioners towards what defence measures should seek to remedy. If State A's activities threaten the likelihood of State B coming to the aid of her ally, State C, then any defence measure increasing the likelihood of such aid should be considered. Set generation is here broken down to three main steps – making a selection, producing plausible arguments, and considering the purpose of defence measures – for a more detailed discussion.



The first step is to make a selection of activities to study as possible influence threats. Set generation relies on practitioners selecting foreign influence activities to consider but offers no guidance on how to make a selection. The selection could consist of anything from a single tweet to the entirety of power resources used by the adversary. It could consist of the most recent activities alone or the most updated list of his activities, e.g. the most recent tweets or all activities including the most recent tweet.

This report does not discuss how to best cluster foreign influence activities to understand their implications for state security. We suggest practitioners think carefully through how and why they made their selection, and we encourage experimentation. If the adversary is thinking holistically about the influence effect of his combined use of power resources, it may be fruitful to consider activities both in isolation from one another and as larger clusters. Why consider

only Twitter or social media? Why consider only (dis)information? Why consider only information? Is one form of clustering best for interests in international relations, and another form of clustering best for intrastate interests? We have not been able to find any guidance on how to cluster influence activities for analysis and offer none here. We encourage experimentation, and that the problem be studied further.

The second step is to consider the selection as potential threats to each state security interest as defined. In academic terms, the objective is to create hypotheses as to how the selection of activities inflict harm on each interest in the overview. The result is a set of hypotheses – hence the name set generation. Set generation breaks from academia, however, in that these hypotheses are not tested. Some of them may be true and some may not be. Moreover, they are not necessarily derived in the way academics do (e.g. from a theory). Practitioners must of course investigate the assumptions and implications of their arguments rigorously, but the standards in most cases cannot be as high as in academia to do so at the speeds required for reactive defence. Plausible arguments is therefore perhaps a more fitting name. What matters for defence is that the set of plausible arguments contains a specific subset of arguments: those that are both correct and most harmful to state security. Iterating through a pre-defined overview of state security interests helps ensure the most harmful possible effects are considered, and therefore more likely to be included in the set.

The third step is describing the purpose of defence measures. At this point, practitioners have a set of plausible arguments containing a subset that are both correct and most harmful to state security. We argue states can erect a meaningful reactive defence by defending against the entire set, thus sidestepping the need for exact measurements of effects.

Because the arguments must tie the selection of activities to interests on the map, the arguments themselves also prescribe the antidote. If the selection is potentially harmful to the likelihood of an ally coming to one's aid in a critical situation, the antidote is to improve that likelihood using any power resource at the states' disposal. States can also consider what defence measures are already in place as well as the status of the interests in the overview. It is possible to conclude that no additional defence measures are required, or that a few defence measures are sufficient to protect against a variety of activities.

One fundamental weakness of this approach is that it offers no guidance on how to make a useful selection of foreign influence activities to consider. Another weakness is that set generation is only as good as the overview it is based on. If, for instance, it only considers the outcomes of elections as important to state security, set generation will likely miss other important aspects, such as long-term legitimacy of elections as a democratic institution or a new administration. If the overview is well developed, however, set generation will help practitioners discover the most important aspects.

Finally, one major benefit here is that the overview is created prior to the need for set generation, a lot of the analytical work required to understand the harm from foreign influence is done beforehand. This allows for a quicker assessment, and thus a quicker reaction.

5 Example of implications for defence measures: the creation and maintenance of purposeful narratives

Because this report does not address the problem of using influence, it does not help government practitioners decide how to achieve their goals. The report makes an exception to discuss the creation and maintenance of purposeful narratives as possible defence measures. Narratives are used as a tool to shape how people understand the world around them and clearly also to shape peoples' understanding of international politics. We discuss narratives because we think it useful to showcase what our value-based approach can mean for current practices. Note that we offer no evaluation of their relative importance (i.e. substantial contribution to protecting state security) in a given context.

5.1 What are narratives?

The term narrative refers to the telling of a story or a story line. The field of narrative study emphasizes narratives in all aspects of human interaction, with the assumption that narratives are an integral part of human understanding of the world around them: human beings make sense of the world through narratives. In this sense humans are storytelling beings – tending to think in terms of narratives in order to be able to interpret their surroundings and themselves (Fisher, 1984; Shenhav, 2005, p. 76). This means that every narrative – from an anecdote to a novel to the way history is being taught – shares a common grammar structuring events in a narrative sequence (Khoury, 2017, p. 5). Another characteristic of the narrative is that it cannot be all-inclusive, as this would render it meaningless: «To be meaningful, narratives must select, organize, and prioritize events taken from the raw, unprocessed, and potentially endless list of past and present events» (Khoury, 2017, p. 5). In this lies a necessary bias that is addressed later. A narrative is an expression of a world view – a way of thinking and reasoning resulting in certain perspectives and certain forms of understanding.

It follows from the above description of narratives that they are not simply stories told by one entity and received by another. Narratives are constructed as much by the receiver and by the context in which the narrative is being told as by the teller. The receiver's personality, history, background and experience influence how the story is interpreted, and thus contribute to the narrative. Moreover, the receiver is not necessarily just one person or one homogeneous group. Often, different people or groups interpret the same information differently, thus creating several different narratives. Fisher (1984, p. 2) pointed to these fundamental premises for narrative theory when he wrote that the narrative consists of symbolic words or actions «that have sequence and meaning for those who live, create, or interpret them». Furthermore, narratives are not told through verbal communication only; action, inaction, words spoken, words not spoken – everything that serves to communicate something related to the actor or conflict in question, contributes to the narrative.

Narratives exist to people whether we create them or not, but some are wilfully constructed, skewed or distorted and attempted pushed on others in order to promote a certain form of

behaviour. We can distinguish between narratives that emerge organically as a result of an open dialogue, and thus are formed by all relevant parties in the influence process, narratives that are created by one party pushing this narrative strategically in order to win ground for this understanding, and lastly, narratives that are created strategically by one party in order to manipulate the other. In international politics – and international security politics, especially – states push narratives they perceive beneficial to themselves. As such, state security narratives are strategic in nature.

5.2 A narrative hierarchy

To root narratives in our value-based approach to defence, we require a vocabulary to describe some of the most important narratives with respect to state security. The vocabulary must accommodate certain requirements from this report, such as the interim discussed in section 4.1. Similar vocabularies, such as Nissen's (2014, 2015, p. 47), were discarded in favour of a state-centric adaptation inspired by Roselle et.al. (2014) whose research illustrate a hierarchy of the state's narrative.

In this report, the national narrative is the most basic, and thus at the lowest level of the hierarchy. It is continuous, and defined, over time, partly by the state and partly by the international community. It is an expression of such things as the nation's identity, self-understanding and view of the world around them (Khoury, 2017). Parts of the national narrative concern state security, and those parts are of main interest here. The state security narrative contains such things as what security challenges a state faces, and how it solves them. Due to its importance here, this report refers to that part of the national narrative as the state security narrative.

In this report, there are also three non-continuous narratives: the issue narrative, dispute narrative, and, finally, militarised dispute narrative. They help describe the transitions from peace to armed conflict, and the challenges in managing narratives through them. An issue narrative typically occurs prior to a dispute narrative, because a dispute typically concerns a specific political issue over which conflict develops. Indeed, many issues between states are positive occurrences, or at least neutral, and do not lead to disputes at all. A militarised dispute narrative is required once armed forces begin to play an important part of the dispute, as well as if it escalates further into armed conflict.

Figure 5.1 places the above narratives in a hierarchy. Because states maintain the national and state security narratives in peacetime, and the Y-axis denotes conflict intensity, these two narratives have been positioned below X-axis. An issue narrative inherits from these continuous narratives, and a dispute narrative inherits, in turn, from the issue narrative. Finally, if sufficient intensity levels are reached, a militarised dispute narrative inherits from the dispute narrative. The figure shows an example where an issue arises and escalates into a militarised dispute. In this case, a dispute narrative inherits from the issue narrative immediately, indicating a sharp escalation. Some time after, the dispute becomes militarised. The end of the conflict in this example is not discussed here, and thus not pictured in the figure.

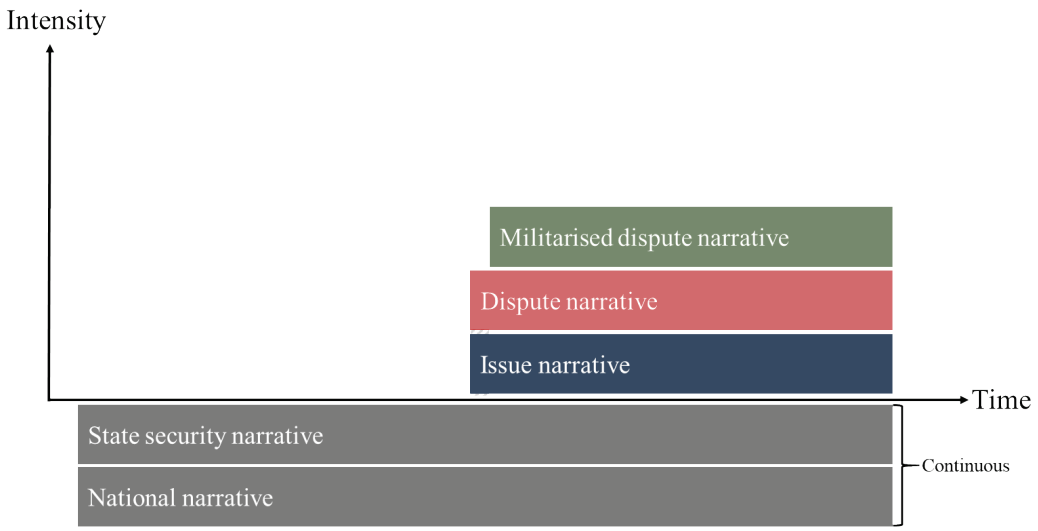


Figure 5.1 A narrative hierarchy.

This narrative hierarchy yields some important insights. The non-continuous narratives are necessarily reactive. They embody what is necessary to protect state security interests with respect to a specific issue. For them to exist, however, governments must detect and acknowledge the issue to begin with. Section 4.1 introduced the notion of an interim, where the target discovers conflict a while after the adversary begun it. The state security narrative is the only narrative in place during an interim, and thus a potential part of a proactive defence during the interim (provided it is shaped with likely contexts in mind).

Figure 5.2 illustrates the above argument. It shows the narrative hierarchy of a state that is the target of unconventional warfare, by superimposing figure 4.1 (see section 4.1) on figure 5.1. In this case, conflict discovery leads to quick escalation adding an issue and dispute narrative at the same time, and shortly thereafter a militarised dispute narrative. During the interim, however, the target's defences against harm in terms of narratives is de facto the state security narrative. If narratives matter to state security in low-intensity conflicts, it seems important to evolve it accordingly.

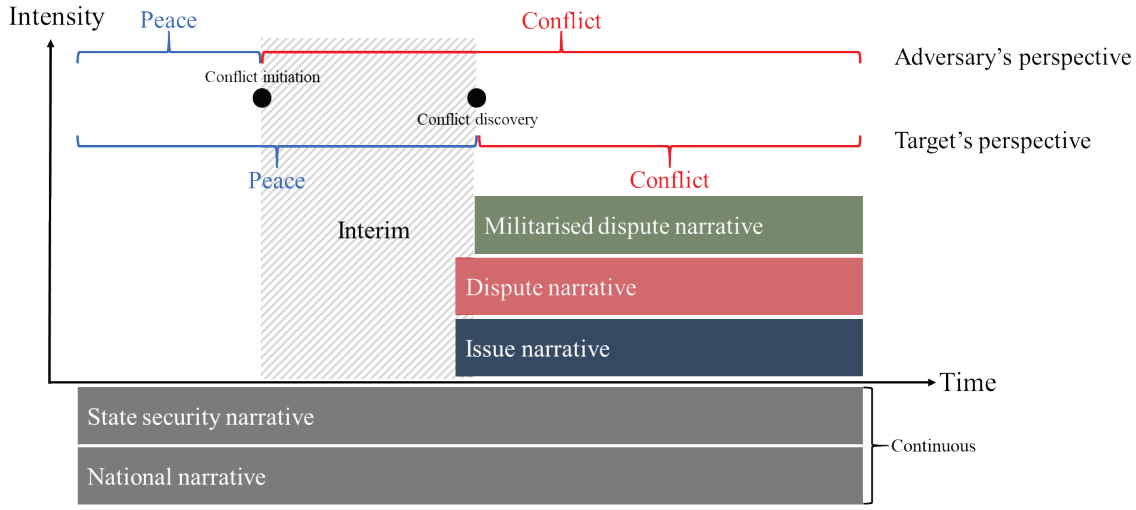


Figure 5.2 A narrative hierarchy with an interim.

Assuming narratives are a significant and substantial part of a defence of state security from foreign influence, the figure highlights the importance of states' continuous peace-time narratives. We therefore continue with a discussion of what our value-based approach means for the maintenance of purposeful narratives.

5.3 On the maintenance of purposeful narratives

Our value-based approach entails the state security, issue, dispute, and militarised dispute narratives should all serve state security interests. It means states using narratives as defence measures should maintain a set of purposeful narratives that addresses a curated set of interests with respect to a curated set of actors. The actors and interests identified through mapping state security essentials (see chapter 3) will help practitioners understand what narratives should seek to accomplish in a given context, and with respect to specific actors.

Providing a real-world example of a grand strategic narrative built purposefully to support state security is beyond the scope of this report, but a rough estimate for a small, alliance dependent state, such as Norway, is not difficult to imagine. It would likely include such things as:

- Domestic support for alliance-membership.
- Domestic support for the defence spending required to maintain that framework, and, implicitly, the costs of relevant national armed forces.
- Maximum likelihood of getting support from key allies in scenarios that require it, at the desired point in that scenario.

Narratives exert influence, and are, essentially, offensive tools (even when used for defence). This report does not address how to use influence, only how to derive what states might seek to accomplish with narratives. An interdisciplinary effort is required to understand how to use influence and create or manage narratives to achieve specific state security objectives. The

authors are not aware of fully developed and tested concepts. For instance, there is no reason to assume there will always be overlap between narratives that deliver the desired effect, and those that are acceptable to put forth in a liberal democracy. If a state is unwilling to adopt the narratives that are required to achieve some state security objective, then it effectively accepts an inherent weakness. A decent concept for using narratives includes analyses of that sort. If there are alternate ways of achieving the same objective – i.e. using something other than narratives – states might consider doing so until a more complete understanding is in place.

6 Summary and concluding remarks

This report has argued Western states' need for a well-functioning approach to defence against foreign influence is much greater today than it was only a decade or two ago. Present efforts often rest on ideas, assumptions and practices which have proven conceptually malleable and problematic in the past. This report therefore adopts a more fundamental perspective. It considers the main objective in this problem space to be enabling states and armed forces to use and/or defend against influence. Current ideas, assumptions and practices, such as StratCom, are viewed as (de facto) concepts for influence.

In the above perspective, there exists a set of tasks that any concept for influence must offer a solution for (that includes opting not to solve it). Identifying these tasks is beyond the scope of this report and likewise creating a concept for influence. This report concerns the subject of defence against foreign influence. It describes an approach to three tasks that arguably belong on the list of tasks any concept must offer a solution to:

- Define what constitutes harm.
- Assess what foreign influence harms.
- Describe the objective of defence measures.

We have developed and described a value-based approach to these three tasks. It rests on the two assumptions that the purpose of defence is to protect state security, and that practitioners will likely not have reliable measurements of effect. The latter holds for both the effects of the adversary's activities and those of practitioners' defence measures. The report is therefore rooted in what state security is and how to protect it, rather than in the more common way of looking at an adversary's influence activities. This in turn leads us to use a relational model of power as a theoretical base to structure our approach to defence.

Our value-based approach is in a sense a method waiting to be applied to a specific case. It describes the work to be done, and how to do it, for states to improve their proactive and reactive defence against foreign influence. A combination of skills is required to apply it to a

specific state. Smaller sections may be parcelled out to research communities, but many will require hands-on from policy makers.

6.1 Further research

Chapter 1.2 discusses influence from a more fundamental perspective, or a different level of abstraction, than what is common in this field today. That level of abstraction leads directly to the specification of three tasks to be solved by defence, and therefore yields key information for comparing and testing approaches to defence against one another. Many tasks remain to be described, both for defence and for influence in general, and further research in this direction is arguably very important to the creation, testing, and further development of any concept for influence. Such work could lead for instance to improving or replacing StratCom.

The authors of this report have backgrounds in military science and political science, and the report is heavily influenced by it. The main objective in this problem space is to enable states and armed forces to use and/or defend against influence, and there are likely tasks to that end which cannot be solved or even identified from the authors' disciplines' perspective. Identifying and solving these tasks will require knowledge integration from several fields (e.g. sociology, computer science, psychology, media and communications) (see also Thuv & Duistermaat, 2019). Identifying tasks that must be solved through knowledge integration and using knowledge integration to identify tasks to be solved, are two interesting challenges for the field.

Western states have struggled with foreign influence before, and many of the problems discussed today, including the need to look at it from a more fundamental perspective, have been discussed before. There are sources that point to historical problems with clear parallels today (see for instance Chotikul, 1986; Hartness, 1966; Robinson et al., 2018; United States Senate Committee on Foreign Relations, 1952). A thorough review of the history of the field might reveal why there has not been more progress over the past half century. The authors argue such a study should adopt the above type of more fundamental perspective, rather than adopt any specific idea for scoping (e.g. information warfare, political warfare, information operations and many more).

Section 1.3 describes the importance of a clearly stated purpose of defence. This report considers the purpose of defence to be protecting state security, but the purpose could be expanded to include for instance aspects of societal security. Expanding the purpose of defence may lead to new requirements regarding how to describe effects. Work in this direction may also help solve another shortcoming in this report; the relational model of power used to describe effects in this report is not a perfect fit. There are interests that are either difficult or awkward to describe as behaviours. Stating interests should preferably be expressed as behaviours is an easy way out. The integrity of nation-wide elections, for instance, is obviously important for international relations. Defining the exact behaviours, and placing them in specific power relations, is both difficult and awkward, and may lead focus away from the simple fact that it is important other states see nation-wide elections as legitimate.

Section 4.3 on set generation raised the question of how influence activities should be clustered. This is an interesting question, and one way of looking at it could be to use a set of interests like those defined in this report. Activities could be clustered in terms of which are expected to be of most utility in achieving a given effect.

Section 2.1 mentioned the challenge of setting reasonable requirements for the argument practitioners put forth to conclude foreign influence is harmful, and thus require defence measures. This report only broaches this topic (in chapter 4.), where no specific requirements are given for reactive defence (i.e. set generation). A combination of institutionalised knowledge and skills (e.g. practitioners' feel for how behaviours are impacted by disinformation) is likely to be used during set generation. Knowledge bases could be considered for this, and perhaps tailored to the types of behaviours that have been defined by a given state.

This report has looked exclusively at states, and defence for the purpose of protecting state security. This is a natural starting point as it forms the superstructure for military operations, but a similar look at defence from the armed forces' point of view would be a natural expansion of this report. Armed forces' values likely lie in their operations, which, in part, are also instruments in direct support of policy.

References

Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections: The Quarterly Journal*, *15*(1), 5–31. https://doi.org/10.11610/Connections.15.1.01

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, *31*(2), 211–236. https://doi.org/10.1257/jep.31.2.211

Alme, V. (2019a). *Falske nyheter som sjanger.* FFI-rapport 19/00660. Kjeller: Forsvarets forskningsinstitutt.

Alme, V. (2019b). *Småstatsnarrativ i internasjonale operasjoner: Sikkerhetspolitiske rammebetingelser og tilsynelatende irrasjonelle valg.* FFI-rapport 18/00223. Kjeller: Forsvarets forskningsinstitutt.

Barger, W., & Barney, R. D. (2004). Media-Citizen Reciprocity as a Moral Mandate. *Journal of Mass Media Ethics*, *19*(3–4), 191–206.

Bergh, A. (2019). *Social network centric warfare – understanding influence operations in social media.* FFI-rapport 19/011194. Kjeller: Forsvarets forskningsinstitutt.

Biersteker, T. (2002). State, Sovereignty and Territory. In *Handbook of International Relations* (pp. 157–176). https://doi.org/10.4135/9781848608290.n8

Bjørnstad, A. L. (2019). *Understanding communication and influence in a defense context—A review of relevant research from the field of psychology.* FFI-rapport 19/01224. Kjeller: Forsvarets forskningsinstitutt.

Boghardt, T. (2009). Soviet Bloc Intelligence and Its AIDS Disinformation Campaign. *Studies in Intelligence*, *53*(4), 1–24.

Brooks, R. E. (2009). *A (Very) Short* History of 'Strategic Communication'*. Retrieved from https://web.archive.org/web/20121224064815/http://www.foreignpolicy.com/files/fp_uploaded_documents/121206_power.pdf

Brooks, R. E. *Ten Years On: The Evolution of Strategic Communication and Information Operations since 9/11".* , § House Armed Services Sub-Committee on Evolving Threats and Capabilities (2011).

Brooks, R. E. (2012, December 6). Confessions of a Strategic Communicator. *Foreign Policy*. Retrieved from http://foreignpolicy.com/2012/12/06/confessions-of-a-strategic-communicator/

C. Marvin, & Meyer, P. (2005). What kind of journalism does the public need? In G. Overholser & K. H. Jamieson (Eds.), *The Press* (pp. 400–411). Oxford, UK: Oxford University Press.

Chen, A. (2015, June 2). The Agency. *The New York Times*. Retrieved from http://www.nytimes.com/2015/06/07/magazine/the-agency.html

Chotikul, D. (1986). *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study:* https://doi.org/10.21236/ADA170613

Dahl, R. A. (2005). What Political Institutions Does Large-Scale Democracy Require? *Political Science Quarterly*, *120*(2), 187–197.

Daniels, L. (2017, September 27). Russian Active Measures in Germany and the United States: Analog Lessons From the Cold War. *War on the Rocks*. Retrieved from https://warontherocks.com/2017/09/russian-active-measures-in-germany-and-the-united-states-analog-lessons-from-the-cold-war/

Diesen, S. (2018). *Lavintensivt hybridangrep på Norge i en fremtidig konflikt.* FFI-rapport 18/00080. Kjeller: Forsvarets forskningsinstitutt.

Eide, M. (2011). *Hva er journalistikk*. Oslo: Universitetsforlaget.

European Council. (2015, March 20). *European Council conclusions, 19 and 20 March 2015*. Retrieved from http://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/en/pdf

EUvsDisinfo. (2018, March 8). Removal of three cases further to complaints by Dutch media. Retrieved 12 March 2018 from https://euvsdisinfo.eu/removal-of-three-cases-further-to-complaints-by-dutch-media/

EUvsDisinfo. (2019). About. Retrieved from https://euvsdisinfo.eu/about

Fisher, W. R. (1984). Narration as a human communication paradigm: The case of public moral argument. *Communication Monographs*, *51*(1), 1–22. https://doi.org/10.1080/03637758409390180

Garmazhapova, A. (2013, September 9). Где живут тролли. Как работают интернет-провокаторы в Санкт-Петербурге и кто ими заправляет. *Novaya Gazeta*. Retrieved from https://www.novayagazeta.ru/articles/2013/09/09/56265-gde-zhivut-trolli-kak-rabotayut-internet-provokatory-v-sankt-peterburge-i-kto-imi-zapravlyaet

Greenberg, A. (2017, May 9). NSA Director Confirms That Russia Really Did Hack the French Election. *WIRED*. Retrieved from https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

Habermas, J. (1993). *The Structural Transformation of the Public Sphere. An Inquiry into a Category of Bourgeois Society* (5th ed.). Massachusetts: MIT Press.

Haines, J. R. (2015, February 17). *Russia's Use of Disinformation in the Ukraine Conflict—Foreign Policy Research Institute*. Retrieved from https://www.fpri.org/article/2015/02/russias-use-of-disinformation-in-the-ukraine-conflict/

Hartness, W. M. (1966). Social and Behavioral Sciences in Counterinsurgency. *Military Review*, *46*(1), 3–10.

Hoffman, F. (2016). The Contemporary Spectrum of Conflict. Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War. In D. L. Wood (Ed.), *2016 Index of U.S. Military Strength* (pp. 25–36). Retrieved from http://index.heritage.org/military/2016/essays/contemporary-spectrum-of-conflict/

Intelligence Community Assessment. (2017). *Assessing Russian Activities and Intentions in Recent US Elections* (No. ICA 2017-01D). Retrieved from Office of the Director of National Intelligence website: https://www.dni.gov/files/documents/ICA_2017_01.pdf

Jamieson, K. H. (2018). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know*. New York, NY: Oxford University Press.

Jones, J. P., & Baym, G. (2010). A Dialogue on Satire News and the Crisis of Truth in Postmodern Political Television. *Journal of Communication Inquiry*, *34*(3), 278–294. https://doi.org/10.1177/0196859910373654

Kennan, G. (1948, May 4). *Policy Planning Staff Memorandum*. Retrieved from http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm

Khoury, N. (2017). Political Reconciliation: With or Without Grand Narratives? *Constellations*, *24*(2), 245–256. https://doi.org/10.1111/1467-8675.12237

Levin, D. H. (2016). When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results. *International Studies Quarterly*, *60*(2), 189–202. https://doi.org/10.1093/isq/sqv016

Lov om nasjonal sikkerhet (sikkerhetsloven) (2018). Retrieved 23 January 2019, from https://lovdata.no/dokument/NL/lov/2018-06-01-24

McNair, B. (2009). Journalism and Democracy. In K. Wahl-Jorgensen & T. Hanitzsch (Eds.), *The Handbook of Journalism Studies* (pp. 237–249). New York: Routledge.

McQuail, D. (2003). *Media Accountability and Freedom of Publication*. Oxford ; New York: Oxford University Press.

NATO. (2014, December 19). *MC 0422/5 NATO Military Policy for Information Operations*. North Atlantic Military Committee.

Nissen, T. E. (2014). Strategizing NATO's Narratives. In L. Odgaard (Ed.), *Strategy in NATO: Preparing for an Imperfect World* (pp. 157–171). https://doi.org/10.1057/9781137382054_11

Nissen, T. E. (2015). *#TheWeaponizationOfSocialMedia: @Characteristics_of_ Contemporary_Conflicts*. Royal Danish Defence College.

Norwegian Ministry of Defence. (2015). *Unified Effort. Expert Commission on Norwegian Security and Defence Policy*. Retrieved from https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/unified-effort.pdf

Nye, J. S. (2011). *The Future of Power*. New York: Public Affairs.

Paul, C. (2011). *Strategic Communication: Origins, Concepts, and Current Debates*. Santa Barbara: Praeger.

Paul, C., & Matthews, M. (2016). *The Russian 'Firehose of Falsehood Propaganda Model'. Why it Might Work and Options to Counter It.* Retrieved from RAND Corporation website: https://www.rand.org/pubs/perspectives/PE198.html

(PO(2009)0141. (2009). *NATO Strategic Communications Policy*.

Robinson, L., Helmus, T. C., Cohen, R. S., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2018). *Modern Political Warfare*. RR-1772-A. Retrieved 11 April 2018, from https://www.rand.org/pubs/research_reports/RR1772.html

Roselle, L., Miskimmon, A., & O'Loughlin, B. (2014). Strategic narrative: A new means to understand soft power. *Media, War & Conflict*, *7*(1), 70–84. https://doi.org/10.1177/1750635213516696

Shenhav, S. R. (2005). Thin and thick narrative analysis. On the question of analyzing political narratives. *Narrative Inquiry*, *15*(1), 75–99.

Sjøvaag, H. (2018). Journalism's Social Contract. *Oxford Research Encyclopedia of Communication*, 1–19.

Sodaro, M. J. (2008). *Comparative Politics. A Global Introduction* (3rd ed.). Boston: McGraw-Hill.

Street, J. (2011). *Mass media, politics and democracy* (2nd ed). New York: Palgrave Macmillan.

Tatham, S., & MacKay, A. (2011). *Behavioural Conflict: Why Understanding People and Their Motives Will Prove Decisive in Future Conflict*. Saffron Waldon, Essex, U.K: Military Studies Press.

Thuv, A., & Duistermaat, M. (2019). The Military In A World of Pervasive Influence. In *STO Technical Report*: *Vol. AC/323(SAS-117)TP/879*. *Emerging Threats in the Information Environment*. NATO Science and Technology Organization.

United States Senate Committee on Foreign Relations. (1952). *Overseas Information Programs of the U.S. :hearings before the United States Senate Committee on Foreign Relations, Subcommittee Under S. Res. 74 on Overseas Information Programs of the U.S., Eighty-Second Congress, second session.* Retrieved from http://hdl.handle.net/2027/umn.31951d02094637q

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

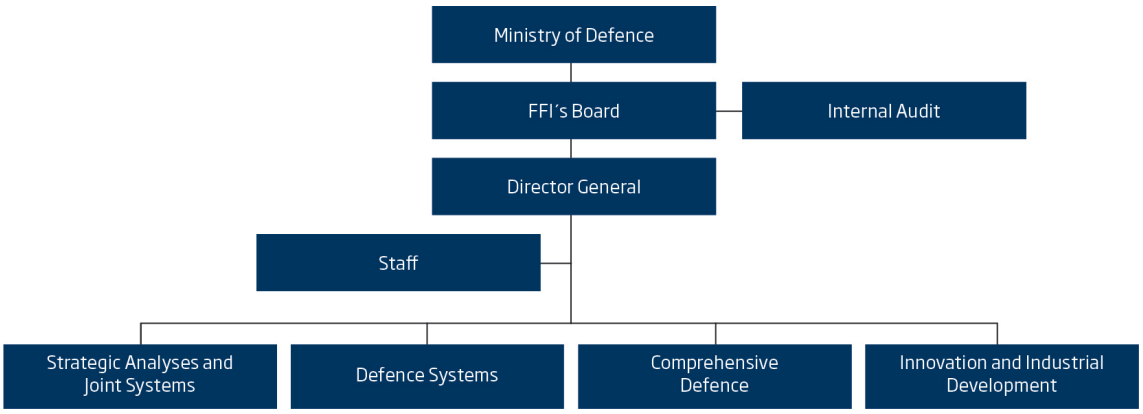
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment