2014

SWEDISH DEFENCE UNIVERSITY

Coercive instruments in the digital age:

The cases of cyber-attacks against Estonia and Iran

Swedish National Defence College

Department of Security, Strategy and Leadership

Political Science with a focus on Security Policy Fall 2014

Mentor: Ronnie Hjort

Abstract:

In the wake of the cyber-attacks in 2007 against Estonia and in 2010 against Iran, academics have debated the character of cyberwar. This study applies the theories of coercive diplomacy to the cases of Estonia and Iran in order to explain cyber-attacks as instrument for coercive diplomacy. While the long term effects of the attacks have yet to be understood it is clear that cyber-attacks can, and will, become a serious threat against political decision-makers in times of conflict.

Key words: Coercive diplomacy, cyberwar, cyber-attack, Stuxnet, DDoS, hacktivist

Contents

Introduction

In recent years the use of information technology in political conflicts has gained increasing attention. As society becomes more reliant on IT infra-structure, security experts as well as politicians are becoming increasingly concerned regarding this new vulnerability.

The exploitation of weaknesses in systems or computer networks, hacking, and malicious computer code, computer viruses, have come to move from being a nuisance with potential economic damage to a threat to national security. Since then, numerous attempts have been made to explain, and fit, cyber-attacks in existing frameworks explaining political conflict.

One major debate is whether or not cyber-attacks can be significant tools in warfare, if there is such a thing a *cyberwar*. In 2012, Thomas Rid published an article, later to be fleshed out into a book, where he argued that the character of cyber-attacks did not fulfil the definition requirements of war, which include direct lethal effects.

In this essay, the aim is to test if the theories of coercive diplomacy can be applied on the use of cyber-attacks during political conflict.

In order to do so, there is a need to understand the nature of cyber-attacks as well as the concept of coercive diplomacy as a political tool. By studying contemporary theories on the use of political force, one can start to understand in what way cyber-attacks can pose a threat to national security and harm society.

Cyberwar is coming!

The notion that cyber-attack would someday come to be a threat to national security is far from new. Well over 20 years ago, in the article *Cyberwar is coming!* (Arquilla & Ronfeldt, 1993), the authors argue that progress in information technology would change how society handled conflict and warfare. Future wars would take place, in part, in the digital arena.

Arquilla and Dondeldt defined two emerging aspects of conflicts in the digital age: Netwar and cyberwar. Both modes of warfare rely on the manipulation of knowledge. Knowledge about yourself and your enemy is a central part of conflict. Knowing what, where, and why the enemy, as well as yourself, is doing something, is a casual point of any conflict, be it military or political.

Netwar refers to a conflict between nations and societies on a grand level where the belligerents try to disrupt the flow of information. Its aim is to influence the information available to populations, changing what society perceives as truth about itself and the world around it. It is likely a combination of diplomatic efforts, psychological operations, as well as manipulation of information databases. The common factor is the targeting of information and communications, in order to reach its goal. It is unlikely that netwars will be violent, in themselves, but will likely be part of some low intensity conflicts (Arquilla & Ronfeldt, 1993).

Netwar is not only a tool for governments. Non-state actors such as organised criminal syndicates, non-governmental organisations and terrorist organisations will all have motives and means to change information in regards to their interests. Communication and information will increasingly become a factor in organizing and mobilising for a certain cause. Netwar is not limited to interstate conflict, but can be utilised both by, and against, non-state actors in order to legitimize or delegitimize the actor's actions (Arquilla & Ronfeldt, 1993).

Cyberwar is defined as "conducting, and preparing, military operations according to information-related principles." This means disrupting the information and communication systems used for the enemy to organize itself (Arquilla & Ronfeldt, 1993).

The main difference between cyberwar and earlier warfare is that cyberwar depends less on geographic location than other means of warfare. Cyberspace cuts across most nation borders and brings countries, set on different sides of the globe, to merely a few lines of computer code apart (Arquilla & Ronfeldt, 1993).

Cyberwar may also, Arquilla and Dondeldt argue, change the way we wage warfare altogether. The main mode of warfare since the mid 1600 has been attrition, fighting your enemy until his resources are depleted and he is unable to continue, before you could achieve your objectives. Cyberwar may help avoid the need to engage in combat in order to defeat opposing forces. A virtual disruption may lead to the capitulation of the enemy before the need for battle emerges. A strategic cyber strike at the heart of the opponent's information systems may be so crippling that the opponent is unable to mobilise at all.

20 years later (Arquilla, 2013), Arquilla revisited his earlier speculations on cyberwar in a new article, where he acknowledged that cyberwarfare was on the rise although not entirely in the way he and Dondeldt had anticipated two decades earlier.

Arquilla pointed to three incidents as major watershed events in the evolution of cyberwar. The first two came in 2007 and 2008 when Estonia, and later Georgia to some extent, were attacked by systematic cyber-attacks in the wake of conflicts with Russia, making it hard to deny the relevance of the cyber domain in modern conflicts.

The second event was in 2010 when a sophisticated computer worm, Stuxnet, caused major damage to Iranian uranium enrichment centrifuges, proving that malicious computer code can be used to cause physical damage (Arquilla, 2013). Aquila argues that these incidents prove that cyberwar is an important aspect of modern conflict.

In the wake of the attacks on Estonia, Georgia and Iran, as well as some later well-publicised cases of advanced penetrations of critical infrastructure, the debate over cyberwar has gained momentum. Since 2010 many proponents, as well as opponents, have expressed their views and findings both for and against the case of cyberwar.

Cyberwar opens a new domain of warfare separate from others, where new actors can establish dominance, regardless of their relative power in other domains (McGraw, 2013). The relative low cost of establishing cyber strike capabilities may provide a window of opportunity for previously weaker actors to now gain means to deliver striking blows to actors who previously where perceived as militarily stronger (Liff, 2012).

Whether or not one believes that cyberwar will change the dynamics of warfare, attacks on infrastructure have become a reality. It has therefore become important to understand how and why cyber-attacks are used in modern conflicts.

Is cyberwarfare “war”?

Recent academic debate over cyber-attacks has mainly focused on the definition of war and if cyber-attacks constitute an act of war. Thomas Rid is professor of Security Studies at King's College London and have outspokenly criticised the idea that cyber-attacks will ever play a major part of warfare. He argues that the term war is used too casually to describe a conflict situation (Rid, 2013).

Rid cites the classic works of General Carl von Clausewitz, who defines war to be an act undertaken in order to compel your enemy to do your will. Drawing upon this definition of war, Rid determines that war needs to fulfil three fundamental criteria: an act of war needs to be violent, instrumental and political in its nature. Any act that lacks any of these criteria cannot be considered an act of war (Rid, 2013, p. 4).

The first criterion, violence, means that an act needs to be potentially lethal for, at least, one party involved. Violence is the key essence of warfare where violence is escalated until one of the belligerents is defeated (Rid, 2013, p. 2).

The second criterion determines that war also is instrumental in such as it is a *means* to an *end*. Violence without a goal fills no purpose. In order for violence to have meaning, violence is directed as a means in order to compel the enemy to act according to one's end (Rid, 2013, p. 2).

The third criterion is that war is political. Clausewitz wrote, "War is the continuation of diplomacy". The ends, for which war is instrumental, need to have a political motive. The necessity to compel ones opponent arises from a political conflict, wherein a diplomatic resolution was unable to be formed.

Based on these three criteria Rid argues that cyberwar fails to meet the standards of war. Most notably, cyber-attacks have never led to the death of anyone and is unlikely to ever directly result in one (Rid, 2013, p. 32).

Aggression can roughly be divided into a two-part spectrum, with criminal violence on one end and political violence in the other (Rid, 2013, p. 9). On this spectrum everything from ordinary crime to war, the ultimate political aggression according to Rid, can be categorised. Based on this, Rid deducts a few observations:

Criminal violence is almost always apolitical in nature, its motives is enrichment of individuals, not the favouring of a set of political ambitions. War is always political (soldiers display their nationhood openly). In the middle of the spectrum you find political crime, acts that are conducted for political reasons, by nation states, but still considered illegal namely sabotage, espionage, and subversion (Rid, 2013).

For these three sub categories of political aggression, violence is not the main goal. Similarly, the lack of violence and attribution, makes it impossible for a cyber-attack to constitute war. Instead, Rid claims, cyber-attacks are simply another form of political aggression against one's enemies. Rid points out that the perpetrator of sabotage, subversion or espionage, while acting politically, usually have a - at least temporary - interest of avoiding attribution, much like the described cases of cyber-attacks (Rid, 2013, p. 10).

Rid’s claims sparked a few responses, criticizing his conclusions.

Political scientist John Stone wrote in an article, fittingly named *cyberwar will take place!*, that Rid made several unmotivated assumptions, when defining war and the relationship established by Rid between force, violence and lethality.

Clausewitz definition of war does not require the act to be claimed or attributed. Just because history has not presented acts of war without attribution there is nothing to prevent future wars to involve acts of force without attribution (Stone, 2013, p. 105).

Another approach is that of Gary McGraw who, by using the “lowest common denominator” defines war as a “violent conflict between groups for political, economic or ideological reasons” (McGraw, 2013, p. 111)

Like Rid, McGraw divides cyber-attacks into three sub categories: cyberwar, cyber espionage and cyber criminality where they all utilize the dependency on insecure network systems (McGraw, 2013, p. 111). In order to define a cyber-attack as war, McGaw sees the requirement of a consequential kinetic effect. There needs to be a physical impact of the effect. McGraw uses the infection by the Stuxnet worm as an example of a cyber-attack resulting in a kinetic effect: the damaging of the uranium enrichment centrifuges.The debate on whether or not cyber-attacks can constitute an act of war is, in the end, a legal issue. Whether or not cyberwar is real or will happen, it is an undeniable fact that cyber-attacks keep occurring in connection with political conflicts. Many states, amongst them Russia and USA, have adopted defence policies, indicating that a cyber-attack can be considered an armed assault on their territory, and many states have formed their own cyberwarfare units, indicating that cyber-attacks are considered a military matter and are at least perceived as a tool of force. The US department of Defence strategy for operation in cyberspace defines offensive cyber operations as “intended to project power by the application of force in and through cyberspace” (Joint Chiefs Of Staff, 2014, p. 69). Both the White House and officials at the Pentagon have indicated that a strike on US infrastructure can be considered an act of war.[1] Russia has also published its own policy regarding cyber-attacks stressing the threat of attacks targeting vital infrastructure to national security (Russian IT-Review, 2012).

[1] Se for example Gorman, S. and Barnes, J. (2011). Cyber Combat: Act of War. *Wall Street Journal*. [online] Available at: http://www.wsj.com/news/articles/SB10001424052702304563104576355623135782718?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304563104576355623135782718.html [Accessed 26 Dec. 2013].

While the definition of cyberwar has been heavily debated and many attempts to categorize cyberwar into new definitions of generational warfare (Reed, 2008) (Betz & Stevens, 2013) (Liles, 2007) little attention has been given to the impact of cyber-attacks on political decision-making.

The theory of coercive diplomacy defines that, if force is used in order to inflict suffering on your adversary in order to compel him/her into an act, then coercive diplomacy is employed. Any violence for political gain, shy of war, or brute force, can be considered coercive diplomacy.

Research goals

Leaving the legal question on whether or not a cyber-attack can be regarded as an act of war, this essay will instead apply the theory of coercive diplomacy on politically motivated cyber-attacks in order to examine whether or not cyber-attacks can be used as an instrument for political coercion. This essay will focus on two questions. The first deals with the fundamental question: *Can cyber-attacks be used as a tool in order to compel an adversary to conform in accordance to political goals?* How can we understand the phenomena cyber-attacks?

The second question deals with the effectiveness of cyber-attacks. Can cyber-attacks be comparable to other coercive instruments, previously proven to be effective, such as limited strikes or economic warfare? *How effective are cyber-attacks as instruments for conducting coercive diplomacy?*

The theory of coercive diplomacy defines that, if force is used in order to inflict suffering on your adversary in order to compel him/her into an act, then coercive diplomacy is employed. Any violence for political gain, shy of war, or brute force, can be considered coercive diplomacy.

Theory of Coercive diplomacy

The concept of coercive diplomacy

In the 1966 book *Arms and Influence* (Schelling, 2008 [1966]), political scientist Thomas Schelling discusses the use of force in inter-state conflict. The traditional approach to conflict, where the goal is to defeat your enemy with brute force and then coerce him to act according to your term, is defined by Shelling as war. By amassing an army that is stronger than your opponent's, you can secure the object of conflict, or deny it to your opponent - may it be resources, territory or any political action. The traditional notion on military capability in liberal democracies was therefore that an army was maintained to deter foreign actors to attack or intervene in homeland affairs. The army's primary function was to be large enough, that the cost to an opponent, of open conflict, would be too large and therefor would be a deterrent for any potential invaders. To win a conflict, the military might needed to be greater than the opponents military might, in order to weaken him militarily and afterwards force him to do one's bidding.

However, Schelling argues, military might can also be used in a different manner. The result of military action usually leaves destruction and suffering in its wake. The cost of a military operation will always be both economic and emotional. Harm, pain and suffering, which cannot be disregarded and will always affect all parties in a conflict to a lesser or larger extent, is an undeniable part of armed struggle. The decision-makers will therefore strive to avoid drawing harm, pain and suffering upon their own population and upon themselves (Schelling, 2008 [1966]).

Knowing this, a nation can draw upon the fear of harm itself, in order to influence its opponents. In addition to weakening the enemy militarily, force can be used to cause harm, pain and suffering. Military might, Schelling argues, can destroy value as well as protect it. Harm, pain, suffering, or the destruction of value, has never been a primary military objective in itself. Rather it is purely incidental to the main goal of defeating the enemy (Schelling, 2008 [1966]).

Suffering, however, will not achieve anything in itself, as traditional brute force will. Causing pain to the enemy is not the same as destroying the enemy. Suffering is effective when it is held in reserve. Latent violence, and the threat of more to come, will make an opponent act in such a way as to avoid further suffering. Knowing this, a threatening power can make an opponent act in a way that is determined by the threatening power. While brute force seeks to overcome the enemies' strength, latent violence seeks to influence the enemies' motives.

By using suffering, or rather exploiting the wish to avoid suffering, one can make others change their behaviour without the need to defeat them first. By using the mere threat of suffering, opponents will act to avoid it. By making them know that certain actions will result in damage, political goal can be reached, without the need to commit to the total destruction of the enemy. The goal of military strategy no longer has the aim to defeat the enemy in combat but rather to persuade the enemy that hostilities are futile (Schelling, 2008 [1966]). Shelling compares this to the difference between *taking* what you want and *making* someone give you the same thing (Schelling, 2008 [1966]). Schelling called the use of force in this manner *coercive diplomacy* as opposed to traditional warfare, which he called *brute force*.

In order to compel your enemy, the use of force is focused to maximise the harm to a hostile actor rather than as blunt force. By focusing on causing suffering to the enemy rather than to meet the enemy head on, you can defeat the enemies' willingness to fight, without having to commit a large enough force to destroy his army.

This notion changes the dynamics of deterrence. While opposing military strength will cancel each other out, suffering does not. This challenges the traditional approach to military might, which proposed that a large enough army would protect society from harm.

Effective coercive diplomacy

Alexander L. George expanded upon the framework of coercive diplomacy, to which Schelling has established the groundwork. By starting from Schelling's work, George defined the aim of coercive diplomacy as "to create in the opponent the expectations of costs of sufficient magnitude to erode his motivation to continue what he is doing" (George, 1997, p. 5). The strength of the opponent's motivation not to comply is therefore not dependent on military strength alone, but also what is demanded.

Coercive diplomacy differs from deterrence by the fact that it is a response to a specific action undertaken by an adversary, rather than a generic defence strategy (George, 1997). It is therefore important to establish the key elements, which are at stake in order to formulate an effective strategy. Limiting the demands to what is vital for one's own interests, ensures that there is an asymmetry in interests between the coercing nation and the targeted nation. By limiting what is at stake, the probability is higher that a target will succumb to diplomatic coercion, since the perceived stakes do not motivate the latent suffering that the target nation risk.

Unlike war, coercive diplomacy relies heavily on communication (George, 1997). It is just as important that your opponent understands what you are doing and why, since the aim is to change his course of action before you commit all your resources. Coercive diplomacy utilises both words and action as a form of communication. Political demands, threats and deadlines need to be backed up by convincing actions in order to convey a sense of urgency and credible threat. Coercive diplomacy relies both on the clear communication of the threat as well as the target deems that the threat is credible.

George also points out that there are many variables affecting coercive diplomacy as well as which strategy is used are context-dependent. Many factors, including the post-crisis relationship, affect which strategies, threats and time constraints that are available. He lists seven conditions which favours, but not guarantee, effective coercive diplomacy:

Clarity of the objective

Coercive diplomacy works by making your target do what you want. Clarity of the objective and consistency of the demands conveyed to the target gives a clear instruction which to follow in order to avoid punishment. While contributing to successful coercive diplomacy, George notes that clarity is not always necessary or even desirable. Sometimes it is advantageous not to make ones demands too specific or too precise, so that one can remain flexible as to what is a desired change in a target’s behaviour. However, unclear objectives make communication more difficult and will make it more difficult to convey a means for the target to avoid the threatened punishments, lowering the chance of a successful coercive diplomacy (George, 1997, p. 76).

Strength of motivation

In order to convey a credible threat it is essential for the coercing power to be sufficiently motivated by what is perceived as at stake. Without sufficient motivation any action undertaken by the coercing power will not be perceived as threatening enough influence the decision-making of the target (George, 1997, p. 77).

Asymmetry of motivation

Motivation is a function of the interest and values perceived to be at stake and the level of costs one is prepared to accept to achieve ones goal. Since coercive diplomacy is a clash of interests, motivation will be two-sided. The advantage of ignoring the demands may very well be deemed high enough to endure any punishment the coercing part is threatening (George, 1997, p. 77).

Motivation also factors into the actions undertaken by the coercing part and can be exaggerated. However there are limits to how much interests can be exaggerated in order to impress the target.

Sense of urgency

Without creating a sense of urgency it is hard for the target to perceive the threatened latent violence. The coercing power needs to generate a sense of urgency for compliance in order to motivate the target to comply (George, 1997, p. 77).

Adequate domestic and international support

Various examples highlight how domestic as well as international support for a cause, or at least lack of open opposition to the policies contribute to the credibility of the issued threats (George, 1997, p. 78).

Opponents' fear of unacceptable escalation

An opponent often has its own motivation to undertake the actions which clash with one's own agenda, and likely will be willing to suffer some consequences for that action. Understanding where the limit goes for the opponent is crucial for successful coercive diplomacy. A threat means nothing if it is anticipated and deemed acceptable by the targeted party. The threat needs to instil in the target a fear of unacceptable escalation, in order to force the opponent to act to avoid it (George, 1997, p. 79).

Clarity concerning the precise terms of settlement of the crisis

The last of George's conditions, is somewhat related to the first, having a clear objective. George differs between clarity conveying the precise terms of settlement with clarity of demands and objectives. It may be necessary to establish procedures and terms for the cessation of hostilities and safeguards that no further aggressive acts will be performed by the coercing party (George, 1997, p. 80).

George stressed that not every variable is equally important for the success of coercive diplomacy, the most important factors relate to the opponents perception of the situation. The opponent needs to perceive that there lies an asymmetry of motivation in favour of the coercing party, that there is an urgency to comply with the demands and that there is nothing to prevent the coercing party from escalating the conflict to a level which is unacceptable for the target nation. The factors are psychological in nature and work with the perceptions of the targeted decision makers. A great deal of uncertainty is introduced into efforts to ensure success of coercive diplomacy against a particular opponent.

Mechanism of coercive diplomacy

Political scientists Daniel Byman and Matthew Waxman discuss the limits and application of military might (Byman & Waxman, 2002). They argue, that coercive diplomacy shouldn’t be viewed as a single political action where a state issues a threat and another state reacts to that threat by resisting (the coercion failed) or backing down (the coercion was successful). Instead coercive diplomacy needs to be viewed as a succession of moves and countermoves in a dynamic process between two parties in conflict. A coerced nation will not simply accept the threat but move to minimize the impact of the threat. This can be done in two different ways: One can either negate the effect of the threat or impose a greater cost for the coercing nation to execute the threat.

The dynamic process of coercive diplomacy also makes it harder to determine the effect of a single action. A coercive act will prompt the target state to counteract either submitting to the demands or, counter acting with its own coercive move. Coercion is a dynamic contest with both actors often employing coercive acts over time (Byman & Waxman, 2002, p. 37).

The way to implement effective coercive diplomacy is to have the ability to increase the threatened costs to the adversary, while denying the adversary the opportunity to negate those costs or to counter escalate. Byman and Waxman call this *escalation dominance*.

In order to attain escalation dominance, the coercing nation needs to find areas that are sensitive to the adversary and that the coercer can effectively threaten. *Pressure points* vary from nation to nation and are dependent on a variety of factors such as the form of government (democratic nations differ from dictatorships), economic, health, diplomatic relations, and so forth. It is also important to note that pressure points, same as the conditions George set forth, are political and psychological in nature. That means that the most important factor is that the pressure points are perceived as pressure points. It is not enough that the target nation has a vulnerability. The vulnerability has to be perceived as important enough so that the nation will go out of its way to avoid damage. Susceptibility to a pressure point may differ from the most obvious vulnerabilities.

Overwhelming force is not always preferred. If the perceived threat is too costly the threat might backfire prompting the leadership of the targeted country to cease any diplomatic talks in order to not loose public support. This is especially true when the threats are made public (Byman & Waxman, 2002). When coercive acts backfire, Byman and Waxman calls it *over coercion.* This means that even though the instruments employed by the coercer is effective against the target, the outcome is far from what was intended

While George focused on the political conditions which favoured effective coercive diplomacy, neither he, nor Thomas Schelling approached the subject of what instruments where available for an effective coercive strategy. Authors Byman and Waxman focus on the mechanism and instruments of coercive diplomacy. The authors note that causing suffering alone does not necessarily have a coercive effect. Suffering must be dealt in such a way that the suffering has a political effect (Byman & Waxman, 2002, p. 27).

The process of coercive diplomacy works by implementing *instruments* of political coercion in order to strike at certain *mechanisms,* which will result in a coercing effect. The instrument is the threat (or infliction of costs), the mechanism is the way the threat generates the adversary’s concession (Byman & Waxman, 2002, p. 48). They suggest several such instruments: Air strikes, invasions and land grabs, threats of nuclear attack, sanctions and isolation, and support for insurgency.

Air Strikes have been extensively used in US foreign policy when a coercive strategy is invoked. Air strikes are especially effective when the objective is to deny the target nation achieving military objectives. It can be targeted at key installations that are critical for the target’s ambitions, without the need of committing a large ground force (Byman & Waxman, 2002, p. 90).

Another military approach is invasions and land grabs. Ground forces remain the most employed heavily relied instrument for coercion, this is especially true for countries which cannot rely on air dominance in order to carry out air strikes as noted above (Byman & Waxman, 2002, p. 99).

The use of invasion and land grabs as a coercive instrument presents a theoretical problem. The aim of coercive diplomacy was, according to Schelling, the avoidance of brute force. Byman and Waxman acknowledge that the lines between brute force and coercive diplomacy, in the case of invasion and land grabs, often are blurry (Byman & Waxman, 2002, p. 100). The main difference between coercive diplomacy and brute force in this case, is the motivation of the attacker. Invasion can be used as brute force, when it is perceived that negotiations will go nowhere. In these instances, the military objectives are independent of the target nations counter moves. With brute force there are no political actions the target nations can undertake, save unconditional surrender, which can stave off the invasion. If, however, the aim is to use the invasion to exert political pressure, the act should be considered coercive diplomacy, not brute force (Byman & Waxman, 2002, p. 100).

The third instrument, Byman and Waxman propose is the threat of nuclear attack. While almost certainly the most effective tool in regard of inflicting suffering, the authors concede that there are many factors which limit the applicability of nuclear threats (Byman & Waxman, 2002, p. 102).

The fourth instrument is sanctions, or economic warfare. Boycotts, trade embargos and blockade are all tools which are not military, but target a nation's economic capacity (Byman & Waxman, 2002, p. 106f). Sanctions differ from the other tools in that it needs almost exclusively the support of major powers and neighbouring states in order to succeed. If capital and markets can be replaced form other sources not partaking in the sanctions, the effects will be very limited (Byman & Waxman, 2002, p. 106).

The final instrument, the authors discuss, is support for insurgency (Byman & Waxman, 2002, p. 117). Support to local insurgency's can be used to deny victory to the adversary's or to destabilise the country (Byman & Waxman, 2002, p. 118f).

Coercers seldom rely on one instrument to achieve its goal. Combinations of the tools are used in the dynamic process, which is coercive diplomacy, as outlined above. These instruments are employed when the coercer want to exploit one, or several mechanism, which cause concession.

Byman and Waxman outline a few mechanisms: *power base erosion*, threatening a regime's relationship with key supporters, *unrest*, creating popular disaffection, *decapitation,* threatening the leadership's personal security, *weakening*, debilitating the country as a whole and *denial*, preventing military and/or political victory (Byman & Waxman, 2002).

Methodology

The logic of cyber-coercion

The available cases of politically motivated cyber-attacks are few and the use of the instrument is in its infancy. A major problem in researching cyberwar is the problem of attribution. As stated above, cyber-attacks are notably seldom attributed with a 100% certainly to a specific actor (even though, for most part, a very plausible suspect is quickly identified). However, attribution is not as important as it may first seem.

Byman and Waxman outlined cases where coercion is not perpetrated by the principal actor but can also be performed by, and with, allies and other actors sympathetic to ones cause. By disregarding the actual perpetrator and focusing instead on which party gained from the act, and which party suffered from it, the question of attribution can be circumvented. Using allies is not uncommon in coercive diplomacy (Byman & Waxman, 2002, p. 152ff). In fact, it may be even to the advantage of an actor that the origin of the attack remains unclear, as long as the demand is effectively conveyed. Counter-escalation is harder to achieve if the attacker is unknown, and plausible deniability may have a deterring effect on the targets ability to counter the attack or motivate counter moves against its allies.

The important factors are the relationship between the attacks and the resulting effect. By focusing on the demands (whether explicit or implied), the gaining party can be determined without establishing who initiated the attack.

Byman and Waxman also pointed out that coercive diplomacy is far from a precise tool or guaranteed to have the desired effect, or indeed any effect at all, on your adversary.

The first question in this study, whether cyber-attacks can be used as a tool of coercive diplomacy, can be approached by examining cases of cyber-attacks and test them towards criteria stipulated by the theoretical basis of coercive diplomacy.

The key component of coercive diplomacy is the use of force to create, or potentially create, suffering, a situation which the adversary wishes to avoid. There is no need for violence or lethality, as long as the actions cause the adversary to strive to avoid the effect of the action. Any tool capable of inflicting suffering, whether it is in form of death, destruction or any other form of cost, can therefore be considered a tool of coercive diplomacy. If a deliberate act results in suffering for an adversary, it is thus a potential tool of coercive diplomacy.

Coercive diplomacy is, for this study, understood as every action where the use of force is employed to compel an adversary to changing political decision-making, as opposed to full-scale war, where the goal is to render the enemy incapable of fighting before attempting to convey any demands.

From such premise, a hypothetical scenario can be established: *A cyber-attack is used in order to cause suffering in a target nation, with the aim to influence political decision-making.*

In this sequence of events three distinct factors can be identified: *(1) The attack needs to be conducted by utilising information technology, (2) the attack needs to be intended to influence political decision-making and (3) the attack needs to inflict suffering.*

The US government defined cyber-attacks as “deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and or/programs resident in or transitions these systems or networks.” (Singer & Friedman, 2014).

Argumentation for the choice of method

Research can roughly be divided into two main fields, qualitative and quantitative. Qualitative research deals with the meaning of the studied phenomena rather than statistical quantifiable data (Alvehus, 2013, p. 20).

A common method for qualitative research is the case study. A case study is used to find an understanding of the interaction between the studied phenomena and context (Iacono, et al., 2011, p. 58). In this essay, case studies are used to test how the cyber-attacks affected the targeted nations and if it can be determined that such attacks had a coercing effect. By studying more than one case, common factors can be determined and the reliability of the theory can be strengthened.

This essay aims to test whether or not cyber-attacks, when used within the context of political conflict, may be understood as an instrument for coercive diplomacy. To test this, two cases of cyber-attacks used in context of a political conflict will be studied, and then compared to similar cases, where cyber-attacks were not used.

This essay utilizes two methodologies:

First, the studied cases (i.e. two cyber-attacks) will be tested against an already established theory. A case study's primary quality is that it is easy to identify and measure the criteria on which the study is founded; it is therefore appropriate for testing already established theories (Esaiasson, et al., 2012). This study can be described as *theory testing* (Esaiasson, et al., 2012, p. 40). For this essay, the question is not how common cyber-attacks are in coercive diplomacy, but rather if they fit the prerequisites for a coercive instrument, and how well they function. A qualitative approach is therefore suitable in testing the theory.

Secondly, in order to distinguish similarities and differences, the cyber-attack cases have been compared with two comparable cases of coercive diplomacy, in which cyber-attacks were not the principal instrument of coercion.

Comparing cases can be done in several ways. Since one goal of this study is to find factors that influence which instruments are employed for coercive diplomacy in a particular situation, it is appropriate to compare similar cases but where the coercing actor used different coercive instruments. By comparing similar cases, which only differ on certain key aspects, common traits can be discerned which may have influenced the choice of strategy by the decision makers. This method is often referred to as “Mill's method of difference” (Theorell & Svensson, 2007, p. 225).

A weakness of case studies is that it may be difficult to isolate the relevant variables which affect the outcome of the studied phenomena, and case studies are strengthened if multiple cases can be studied in a similar way. We have to recognize, however, that the complexity of cases will have a negative impact on the reliability of the findings. The available cases of politically motivated cyber-attacks are, however, few and the use of the instrument is in its infancy.

The limited availability of material and cases to study, makes any approach with a more extensive scope, difficult. Therefor this study can be regarded as a pilot study, and the findings may be significant and useful for further research.

Selection and delimitation of cases

There are several steps when selecting cases for case studies.

First the studied phenomenon population has to be determined. A case can be described as "a phenomenon of some sort occurring in a bounded context" (Miles & Huberman, 1994, p. 25). In this case it is the phenomenon of cyber-attack within the context of political conflict.

The population for this essay is characterised by two factors: *(1) There is a political conflict where coercive diplomacy is employed; and (2) Perpetrator and target are both states.*

After determining the population, cases can be selected for study. There are two main strategies for selecting data for a study: random and strategic selection. In the former, randomly selected cases from the population are studied, and in the later, appropriate cases are selected, based on either the case as a typical (best case scenario) or extreme (worst case scenario) example of the studied phenomena (Esaiasson, et al., 2012, p. 161). For case studies, the most commonly used method is strategic selection. When cases are selected strategically, reliability of the findings can be negatively impacted by selection bias. Therefore it is important to specify how, and why cases are selected.

For the present study, *the first* criterion was that the cases where cyber-attacks where the principal motive was a political conflict. As previous literature points out, cyber-attacks are not only used for political motives. This makes the context of the attacks important. Cyber-attacks can be political, attempting to influence decision-making, or apolitical, often used for monetary gain. In order to sort out apolitical attacks, the aim of the attacks needs to be deduced by examining demands and/or targets for the cyber-attacks.

A second criterion was that national states where the primary actors. The theory of coercive diplomacy is mainly focused on conflict between state actors, so a further delimitation is concentration to conflicts between state actors, or where states are attributed as main actors.

A third criterion for selection was the presence of similar situations, where the coercing actor did not use cyber-attacks as the principal means of coercion.

A fourth criterion, that there was a difference in aim and type of attack, would add to the diversity and significance of the results.

Two primary cases were selected for this study, both with complementary cases with similar situations but with different means of coercion, than cyber-attack. The first selected case was the 2007 DDoS attacks on Estonian IT infrastructure. The coercing is attributed to Russia, and on that assumption a similar case, where Russia resorted to the use of force in order to compel its adversary, can be found in the similar Georgian conflict, where a former satellite state of the Soviet Union tried to build closer ties with EU and NATO, something Russia opposed.

The second selected case was the 2010 attacks on Iranian nuclear enrichment facilities. Israel is attributed as one possible main perpetrator in that attack. A similar attack was conducted by Israel in 2007 against Syrian nuclear installations.

The attacks on Estonia and Iran differ on some key aspects, thus fulfilling the fourth selection criterion. The methodology where radically different: In the case of Estonia, the attacker coordinated activists and computer networks to attack Estonian webservers with distributed denial of service attacks. The attack relied on sheer volume of computer power and required neither high skills with a computer system or familiarity with the targeted computer systems. In the case of Iran, the infection of the Natanz facility with the Stuxnet computer worm required knowledge, both in regards of general skill, as well as familiarity with the target system.

The attacks targeted different groups: in the case of Estonia, a majority of Estonian residents and companies where affected, while in the case of Iran, the virus was written in such a way as to only activate itself once it was certain that very specific computer systems where infected, limiting collateral damage. The attacks on Estonia where carried out publicly, while considerable efforts were made to hide the activity of the Stuxnet worm.

A final factor when selecting cases is purely pragmatic (Alvehus, 2013). While this is not an optimal criterion for selection, it is unavoidable to some degree. The use of cyber-attacks in conflicts is relatively new, and the total number of known cases is limited. In this essay, selection of cases is is based on previously published source material, adding the necessity that there had to be sufficient published data on the cases.

It is worth noting that both cases selected for comparison with the primary cases, also involved aspects of cyber-attacks, but these were employed differently, with the aim to augment kinetic attacks.

Material and Source criticism

The selection of material has been geared to the aim of the study: not to present new data, but to examine if already established facts fit the given parameters of coercive diplomacy.

Selection of material for this study presents certain particular difficulties: the reliability of data concerning politically motivated cyber-attacks is often difficult to assess. As with most studies of political decision-making, there are many incentives to frame the events into a light favouring one’s own agenda, thus affecting the results (Esaiasson, et al. 2012, 285). Furthermore, the clandestine character of cyber-attacks leaves few official records available to analyse.

In order to determine the reliability of source material, the material is evaluated by using the historical method namely by its authenticity, dependency, concurrency and tendency (Esaiasson, et al. 2012, 279).

The material used in this study builds on data published in peer-reviewed journals, academic books, government documents, published technical analyses from security firms, and news articles. Relying on secondary sources provides little control over the authenticity of the primary sources referenced by the studied material. The main material used for this study, however, stems from peer-reviewed articles from academic journals. It is reasonable to expect peer-reviewed articles to be based on material that is adequately independent, concurrent and free from tendency. Academic books, government documents, technical reports, and news articles have, when necessary, been used to complement peer reviewed articles.

Technical reports are cited when there is a need to present technical aspects of the cases (mainly cyber-attacks), and are also deemed to be adequately authentic, independent and free from tendency.The use of government documents and news articles are more problematic when determining independency and lack of tendency, and are therefore used sparingly. When government documents are used, they are not quoted as a statement of fact, but as the representation of the views of the government. News articles are quoted from well-established news outlets. In this study articles from Der Spiegel, Foreign Policy, The New Yorker, Russian IT Review, The Guardian, and Wired have been used.

Material gathered for this study is deemed non-controversial in as such as most academic publications assume that it is plausible. The facts presented in this study are selected based on the agreement of different sources on the authenticity or plausibility of the given fact.

Assumptions, however grounded, will always be assumptions and the fact remains that any evidence in the presented cases are circumstantial. The involvement of state actors has yet to be acknowledged by the states or directly proven. Any evidence presented in this study needs to be seen as the general assumption of the research community, not as an undeniable proof of involvement.

Operationalization

Byman and Waxman write that coercive diplomacy cannot be viewed as a single act and response, but needs to be put into context, where political coercion is combined with other political tools in a dynamic process of acts and counter acts. It should therefore be possible to put the cyber-attacks into a larger context, within a conflict. The demands and/or targets as well as the actions that precede or follow the attack, may provide an understanding of which context the attack should be viewed in.

To test the research questions against the cases, two key factors will be examined.

1. The instrument needs to impose a cost on the adversary
2. That cost needs to effectively trigger a coercive mechanism.

If there was evidence that both criteria where fulfilled, it is plausible that coercive diplomacy was employed or could have been employed and that cyber-attacks can be considered coercive instruments.

Testing for the first criteria is simple: if the act results in any form of physical or economic damage for the target, a cost has been imposed. However it may be in the interest of the target nation to cover up and minimise the public knowledge of the costs for political reasons. An alternative way to measure the effect is by examining the targeted nation's response. Byman and Waxman provide examples of instruments for countering coercive acts. By examining the target of the attack and determining if the attack provoked a response, which either minimised the effect of the coercive act or can be viewed as a counter escalation, it is possible to deduce that the attack inflicted some form of suffering which the targeted nation wished to avoid.

The second criterion is harder to test for. Effectiveness of an action can be measured in two ways. It can either be measured against itself, answering the question, *does the action accomplish its task?* Or it can be compared with alternative solutions answering the question *does it accomplish the task better or worse than any alternative methods?*

In order to test effectiveness both ways, two methods are be employed in this study.

The first is provided by George in the framework of conditions which favours effective coercive diplomacy detailed above. At least some of the factors he suggests should be present if coercive diplomacy is deemed effective, and that should answer the question if an act can accomplish its task.
The second method is to compare the tested cases with similar cases where other coercive instruments where used. By comparing the use of cyber-attacks as coercive instruments with other cases where other coercive instrument where used, this study aims to determine whether cyber-attacks are more or less effective than other coercive instruments.

Byman and Waxman stress that coercive diplomacy should be viewed as a dynamic process and studying coercive instruments without context is problematic. Any results of this comparison cannot be viewed as conclusive, but can give an indication of the factors that determine when and why certain instruments are used.

Case studies

Cyber-attacks on Estonia 2007

After World War II Estonia became part of the Soviet Union, where it remained until august 20, 1991, when Estonia declared independence. A common tactic employed by the Soviet Union, in order to pacify annexed countries, was to move ethnic Russians into the country in and “Russify” the territory, “diluting” the indigenous population with citizens known to be loyal to the Russian regime (Herzog, 2011, p. 50). After the annexing in the late 1940s, hundreds of thousands of Russians where relocated to Estonia. The Russian minority is a sour spot for the Estonian government. Ever since the declaration of independence the russification of Estonian culture was perceived as a threat to Estonian independence and Estonian officials have created legislation with the aim to minimize the impact, and spread, of Russian culture in the country (Herzog, 2011, p. 50).

In 2004 Estonia took further steps away from Russian influence, when the country gained entry into both the EU and NATO. However, Russia still retains a lot of, primarily economic, interests in Estonia, e.g. Estonia is a key country for Russian export of gas and oil to Europe (Herzog, 2011, p. 53).

For Russia, the integrations of Estonia into EU and NATO is both a political and economic problem The Baltic is perceived as part of the Russian sphere of interest and Estonia is leading the region away from Russian influence (Puheloinen, 1999). Since its separation from USSR, Estonia has made huge efforts to adapt the country to western standards. Information Technology is a field where Estonia has become a global leader. Estonia relies heavily on the internet for many aspects of its critical infrastructure. Everything from financial transactions to water supply is controlled via the internet (Herzog, 2011, p. 51). 97 % of bank transactions are online, and 60% of the population use internet in their daily life. Even government bureaucracy is highly dependent on information technology; the IT director at the Estonian Defence Ministry, Mihkel Tammet, refers to the government operations as “paperless government.” (Herzog, 2011, p. 51)

In April of 2007, after much debate, Estonian officials decided to move a Soviet era bronze statue, depicting a Soviet soldier from the centre of Tallinn, the capital of Estonia, to a military cemetery outside of town. The statue, symbolising the Soviet soldiers killed during World War II, was a painful memory of Soviet occupation (Binoy, 2007).

The decision, however, sparked protests among ethnic Russians still living in Estonia, who claimed that it was a move to further marginalize the Russian speaking population (Binoy, 2007). Riots broke out between Russian protestors and Estonian police, resulting in injuries and the death of one protestor.

Kremlin quickly sided with the Russian diaspora and called the movement of the statue a violation of Russian rights. Russia immediately imposed sanctions on Estonia, briefly shutting down the railway between Tallinn and St. Petersburg (Herzog, 2011).

As the physical protests died down on the streets, the conflict moved to cyber-space. On May 9th Russia celebrates Victory-day, the day when Nazi Germany was defeated, and fallen soldiers of the red army are commemorated. The same day, Estonian IT infrastructure where subjected to large-scale cyber-attacks. The attackers employed a method called distributed denial of service attacks, DDoS attacks.

Detailed instructions where spread on Russian speaking online forums for how users could participate in the attacks and thousands of computers were involved in the attack. Some computers participating belong to pro-Russian activists. Others belong to bot-nets, unknowing users whose computers had been infected by malicious code, enabling the attackers to use the computer for their own gain (Wilson, 2008).

Denial of Service attacks works by repeatedly sending data and requests to a targeted computer. As long as the compute is busy by the query, other data cannot be processed. It can be likened with a highway, the more cars (=data), the slower the traffic.
Distributed Denial of Service attacks link attacking computers together to send more data to a target computer. Like highways, the way to combat a lot of data traffic is to build wider roads (=broaden bandwidth). By linking computers - in the case of Estonia, tens of thousands - one can ensure that it is all but impossible to keep traffic moving while the attack is maintained. It is estimated that the networks funnelled traffic that was up to 1000 times the normal amount, effectively causing Estonian internet capacity to grind to a halt (Wilson, 2008).

One of several groups who claimed responsibility for the attacks, was the Nashi (Russian for “ours”). Nashi is a pro-Putin group organising 120 000 Russian youths between 17 and 25. While not part of the Russian government, there are many links between them and the youth group. The assistant of then parliamentary leader Sergei Markov, was the leader of Nashi and openly confirmed his group’s participation in the attacks (Singer & Friedman, 2014, p. 110f).

The attacks continued for nine days, with a final large attack on May 18th, though many institutions still reported minor disturbances after that date. The attacks effectively prevented bank transactions and even the use of teller machines to withdraw cash Only a handful of financial institutions published figures where loses where estimated, but for one single bank the loss amounted to millions of dollars (Herzog, 2011, p. 52).

There is little doubt that the attacks on Estonian websites where connected to the overall tension between the Russian minority and the Estonian government, however experts have failed to produce credible evidence that supports the claim that the Russian government where directly involved in the attack. However many experts in the field point out that the magnitude of the attack would have been impossible if there were not at least some form of coordination and preparation (Herzog, 2011, p. 52). Whatever their involvement in the cyber-attacks, Russia played a key role in mobilising the activists and ensuring that the tensions remained high and many experts are far from convinced that Russian government had nothing to do with the attacks. A NATO official is quoted in saying: "I won't point fingers. But these were not things done by a few individuals. This clearly bore the hallmarks of something concerted. The Estonians are not alone with this problem. It really is a serious issue for the alliance as a whole” (Traynor, 2007).

To counter the cyber-attacks Estonia received help from EU and NATO Computer Emergency Response Teams (CERT) who contributed to restoring the networks to normal operation. At the same time NATO and EU officials began to discuss strategies and policies regarding response to cyber-attacks. The result was a unified NATO policy on cyber defence but, despite German calls for extending Article 5 of the NATO charter to cyberspace, the organization decided against adopting a unified policy treating a cyber-attack as an armed assault (Herzog, 2011, p. 54f).

Limited warfare in Georgia

Georgia is, like Estonia, another former republic within the USSR. In 1921 The Red Army invaded the country, toppling the government and installed a communist government, loyal to Moscow. However opposition to the occupation has been strong since then, resulting in several protests that were violently put down by Soviet troops, the latest one in 1989.

Georgia declared independence in 1991, shortly before the collapse of the Soviet Union, and since then, relations with Russia have been characterised by mutual distrust and tension (German, 2009).

Since the disintegration of the Soviet Union in 1991, the South Caucasus region has become a battleground for geopolitical influence. The main opposing forces are Russia, who strives to maintain its influence, and Turkey, Iran as well as Western powers, seeking to establish influence in the wake of the Soviet collapse (German, 2009).

Following the 2003 “Rose Revolution”, Georgia’s President Mikhel Saakashvili has been more inclined to seek partnership with Western organisations such as EU, NATO and ISCE. Integration with both NATO and EU have been key priorities for the Georgian government, as evident in the country’s National Security Concept, approved by parliament in 2006 (German, 2009, p. 226).

Russia aims to maintain its influence in the South Caucasus, and opposes Georgia’s pro-Western tendencies (German, 2009). Russian president Vladimir Putin has insisted that former Soviet states are part of Russian sphere of interest and has opposed Western entanglement in what he considered Russian “strategic backyard” (German, 2009, p. 229).

Georgia retains, as part of its heritage as a former Soviet state, close dependency on Russia for export and trade, something Russian policy makers have exploited to exert economic pressure on the country. Economic intimidation has proved to be a successful way to exert pressure on Georgian civilians and undermining the government. In 2006, this became evident as Russia imposed a ban on Georgian food exports to Russia, collapsing the Georgian wine market, which exports up to 87% of its produce to Russia. Furthermore Georgia was, until late 2008, heavily dependent on imports of Russian gas (German, 2009, p. 229).

In 2004, when Saakashvili was elected president, he vowed that restoration of Georgia’s integrity would be a priority for his government. Key elements of this would be resolution of the conflicts that had lasted between Georgia and two separatist provinces, seeking either integration into the Russian federation (South Ossetia) or independence (Abkhazia). Both regions had previously fought Georgia in two wars in 1992 and 1993, respectively, which had ended with Russia as an intervening and peace enforcing agent (Allison, 2008, p. 1146).

A substantial part of the inhabitants in the separatist regions are ethnic Russians, a fact which Russia uses to motivate its continued involvement in the region.

95 percent of the population of South Ossetia have Russian passports, the Rouble is the official currency and many key positions in the South Ossetian government are held by current or former Russian officials (German, 2009, p. 233).

In august 2005, Russian foreign ministry confirmed that the statistics in Abkhazia where similar: over 80 percent, had Russian passports, a figure which was expected to rise following a decision in Moscow to only pay pensions, owed from work in former Soviet Union, to those Abkhazians who held Russian passports (German, 2009, p. 334).

Seeds for what would culminate into the August 2008 hostilities where set six months prior in the wake of the EU and US recognition of independence of Kosovo. Russia, an ally of Serbia, was not pleased with the outcome and retaliated by stating that it would recognize the separatist regions of Georgia as a counter move. Russian anger deepened when, during the NATO Bucharest summit in April, it became evident that Georgia, together with Ukraine, had made substantial progress with the negotiations regarding membership in the military alliance (German, 2009, p. 235). As a response, Russia increased its cooperation with the separatist regions, establishing direct official Russian relations with the South Ossetian and Abkhaz authorities.

The situations slowly deteriorated until July 2008, when Georgian villages and military installations where attacked by separatist militia, provoking several serious clashes between Georgian military and Separatist militias (Allison, 2008, p. 1147). Volunteers arriving from Russia where integrated into the standing South Ossetian militia, with little or no reaction from Russia, prompting Georgia to accuse Russia of complicity and being involved by proxy (Allison, 2008, p. 1147). On august 8, confrontations spilled over into open conflict with separatist militia prompting Russia to send in its own troops to assist the separatists.

After three days of open combat between Georgian and Russian military forces, Georgia was forced to withdraw from South Ossetian territory (Allison, 2008, p. 1147).

On August 12 a ceasefire accord was brokered between Russia and Georgia by French president Nikolas Sarkozy. Then Russian president Medvedev declared an end to the Russian offensive, but ordered his troops to remain. Russian military where given instructions to destroy “pockets of resistance and other aggressive actions and Russian government reserved a right to undertake additional security measures deemed necessary by them. Broad buffer zones where established and unilaterally determined by Moscow drawn up as to inconvenience the Georgians, some examples include the inclusion of the only road connecting Eastern and Western Georgia, the Senaki airfield and the entrances to the harbour of Poti, all of whom now would be under direct Russian control (Allison, 2008, p. 1158).

Cyber-attack on the Natanz

The use, and proliferation, of nuclear arms is one of the major security concerns in the world and considerable effort has been made to limit the spread of weapons and know how. The UN non-proliferation treaty established in 1969 binds signatory countries to abandon their nuclear weapons research and in return receives the shared know how of the participating countries civilian nuclear research. Iran signed the non-proliferation treaty in 1969 and ratified it in 1970.

Israel and the USA have, together with allied Western powers, suspected that Iran has re-established its nuclear weapons program and has been pursuing nuclear weapon capabilities since the mid-1980s. The claim has been repeatedly denied by Iranian officials, who insist the Iranian nuclear program is for civilian use only, in accordance with the non-proliferation treaty (Bahgat, 2006, p. 307).

In 2002 the National Council of Resistance of Iran (NCR), an Iranian oppositional force, produced credible evidence that Iran performed undeclared activities regarding their nuclear program (Squassoni, 2006, p. 2). The International Atomic Energy Agency, IAEA, conducted an investigation and concluded that two facilities had been constructed neither with their access nor knowledge. One was the uranium enrichment facility in Natanz (Squassoni, 2006).

IAEA concluded that there was trace evidence of highly enriched uranium, which is mainly used in nuclear weapons. Their findings, together with Iran's reluctance to let IAEA inspectors visit the installations, resulted in a UN resolution demanding that Iran end its enrichment program (UN resolution 1696).

Israel views a nuclear Iran as a potential existential threat and a threat to Israel's strategic edge in the region (Bahgat, 2006, p. 316). While it is not perceived likely that Iran would attempt to use nuclear arms against Israel, the proliferation of nuclear arms might embolden Iran, and Israeli officials fear that the nuclear arms might end up in more radical non state actors' hands.

A possible strike on Iran has been debated for a long time, and in 2004 Israel procured F-161 warplanes, specially build for long range missions, which would put possible Iranian nuclear installations within Israeli operational reach (Bahgat, 2006, p. 317). A potential military strike on Iranian nuclear research would have to deal with several difficulties: (1) a military strike could have a rallying effect on the Iranian regime, strengthening it. (2) Iranian nuclear facilities would be harder to reach than Syria and Iraq since Israel would have to fly over several hostile countries. (3) Iranian nuclear infrastructure is more developed than both Iraq and Syria, making the resilience factor greater than the other two countries. (4) The political fallout of an attack against Iran would worsen the already frosty relationship with other Arab countries. (5) Iran might withdraw from the NPT treaty liming international oversight. (6) Iranian capacity to retaliate is stronger than that of Iraq and Syria (Bahgat, 2006, p. 317).

In late 2009 Russian IT security company, Kaspersky Labs, discovered the first sample of a Trojan virus called Stuxnet (Falliere, et al., 2011). A computer worm is a virus that works by penetrating computer systems and rewriting programs to do the task specified by the worm.

Once Stuxnet had infected a computer it began to search for predetermined programs used to control the centrifuges (Falliere, et al., 2011). The target program of the virus, a program called Simatric WinCC Step7, was the software used to control motors, valves and switches in industrial systems, in this case the uranium enrichment turbines (Zetter, 2011). Most malicious computer code aims to spread its payload as wide as possible, but Stuxnet differed in that respect. The designers put a lot of effort into making sure that the virus only attacked very specific computer environments, limiting the attack to a specific manufacturer and even downloading the specific model numbers on the hardware the program controlled in order to make sure that it was on target (Langner, 2011).

Nuclear weapons require uranium where the ratio of higher isotopes is higher. In order to produce highly enriched uranium, Uranium hexafluoride is injected into centrifuges to separate the heavier isotope from lower yields. In Iran, the facility to do this is located near the city of Natanz in an underground complex housing a few thousand fast rotating centrifuges (Rydqvist & Zetterlund, 2008).

When the program was found, the worm could deliver its actual payload: The virus did two things: First it took over the monitoring system which supervised the turbines and which would have alerted the staff if something was wrong. Instead of reporting what was actually going on with the turbines, the monitoring system would report what the worm had instructed it to report, that everything worked fine. Even if a technician would have performed a system check, the monitoring system would just have reported everything as normal. Secondly, it altered the code handling the acceleration of the centrifuges and made them spin irregularly by accelerating and decelerating the centrifuges repeatedly (Langner, 2013).

The resulting stress was devastating for the centrifuges. IAEA requires plants handling enrichment to make their decommissioned centrifuges available for inspection, to see that no radioactive material is smuggled out. Under normal circumstances, around 10% of centrifuges would need to be replaced annually. The facility in Natanz held around 8700 centrifuges, making 800 replacements per year a normal turn around cycle. But in 2010, within the scope of a few months between 1000 and 2000 centrifuges had to be swapped due to structural damage (Zetter, 2011).

When IT specialists discovered the worm, they were perplexed by its complexity. The worm used previously unknown weaknesses in the source code for different computer systems, so called zero-day vulnerabilities, to propagate and deliver its payload. Out of more than 12 million pieces of malware that antivirus researchers examine over a year, fewer than a dozen manages to exploit a zero day vulnerability (Zetter, 2011). Stuxnet exploited four such vulnerabilities (Murchu, 2010). Symantec, an IT security company, deemed it necessary for the attackers to set up their own mirrored environment, including their own turbines, in order to program the virus as it did, making this an unlikely product of a non-state actor. The code was probably written by at least five different technicians with expert knowledge in different fields, suitable for the design of the virus (Falliere, et al., 2011, p. 3).

Airstrikes on Al-Kibar

Bashar Assad succeeded his father as president of Syria in July 2000. The young, newly elected president (he was 34 when he attained office) initiated several actions which worried the Israeli intelligence community. He supplied weapons to Hezbollah in Lebanon, received high ranking officials from North Kora, and his rhetoric was perceived as more unpredictable than his father's (Follath & Stark, 2009).

In 2006, Israeli intelligence got a breakthrough when they managed to install a Trojan virus, a program designed to give access to computers without permission, on a senior official's computer, while he visited Great Britain (Follath & Stark, 2009). On the computer they discovered colour photographs and documents indicating that the Syrians where constructing a secret plutonium reactor in the Syrian dessert (Follath & Stark, 2009).

The Israelis where concerned about the possibility of a hostile country with nuclear capabilities and consulted the US for a joint strike on the facility. The US, reluctant to repeat a scenario as in Iraq, where weapons of mass destruction had been one of the primary arguments for the attack, wanted to put pressure on Assad in other ways (Makovsky, 2012).

The Israelis where convinced that any talks would just have let Assad buy more time to acquire necessary components and that a limited strike was the only way to stop the program.

The US would not be part of an attack, but agreed not to leak any information or block an Israeli operation, “[Olmert] did not ask Bush for a green light, but Bush did not give Olmert a red light,” (Makovsky, 2012).

Just after midnight on 6 September, 2007, fighter jets originating from Israel headed north-east across the Syrian border and dropped their payload on half built installations hidden in the dessert before returning home to Israel (Garwood-Gowers, 2011, p. 2).

The initial response from Syria was that Israel had penetrated its airspace and dropped bombs in the desert, but without managing to cause any structural harm or human casualties (Garwood-Gowers, 2011, p. 4). Israeli and American officials kept quiet, declining to comment to the media. It would take until almost a year, until April 2008, before Israel and USA publicly confirmed the intended targets (Garwood-Gowers, 2011, p. 6), a North Korean constructed nuclear reactor, which the US and Israel suspected where going to be used for manufacturing nuclear weapons. It was similar to a North Korean reactor well suited for plutonium production (Kreps & Fuhrmann, 2011, p. 173).

The nuclear reactor itself was far from the only key element for nuclear weapon production. Syria lacked several key components for capability to produce nuclear weapons. Syria would still have needed fuel for the reactor to produce plutonium and without a reprocessing facility, which was not available at the Al-Kibar facility, extracting the plutonium from the spent fuel would have been impossible (Kreps & Fuhrmann, 2011, p. 173). The strike negated about six years’ worth of wok, the average time it takes to build a similar reactor as in Al-Kibar (Kreps & Fuhrmann, 2011, p. 173).

The raid furthermore complicated the program, triggering intensive investigations from the IAEA regarding Syria’s nuclear program (Kreps & Fuhrmann, 2011, p. 173). Before the Al-Kibar attack, Syrian activity was more or less uninspected and the facility unknown.

In May 2008, IAEA informed Syria of its intentions to send inspectors to investigate the side at Al-Kibar and review available information. Syria agreed to the demands of IAEA and provided unrestricted access to the site during the visit in June 2008.

IAEA concluded that the site was “similar to what may be found in connection with a reactor site” (IAEA, 2013). It criticised the US and Israel for not notifying the IAEA of their findings and instead decide to act independently. The use of force undermined the due process of verification and rule of law (Garwood-Gowers, 2011, p. 7).

One IAEA diplomat indicated that IAEA took the findings seriously, due to the fact that Syria was on the agenda right behind Iran and North Korea (McElroy, 2008).

Another consequence of the attack is that there are indications that North Korea was less keen to help the Assad regime after the attack (Kreps & Fuhrmann, 2011, p. 175).

Findings

Can cyber-attacks be used as an instrument for coercive diplomacy?

This study used two criteria in order to determine if cyber-attacks could be used as an instrument for coercive diplomacy.

The first criterion is if the attacks resulted in some form of cost, or suffering. In all of the above cases the attacks have resulted in some form of cost.

In the first studied case of cyber-attack on Estonia, there is evidence that the cyber-attacks resulted in substantial costs both in form of damage to the systems and in form of loss of potential profit while the economic system was in deadlock. The few sources that reported costs, show a not negligible cost and the political fallout was massive. In Georgia both the economic sanctions that preceded the hostilities, as well as the subsequent invasion and land grabs, inflicted substantial costs and suffering. Byman and Waxman suggest that weakening or debilitating the country as a whole is effective on countries where leaders are held responsible, and care, for the wellbeing of the country as a whole (Byman & Waxman, 2002, p. 76).

In the second case of cyber-attacks, Stuxnet, exact costs are harder to estimate. The virus did damage the enrichment turbines, increasing the overhead costs. The costs, however, are not comparable to the costs of a total destruction of the facility, as in the case of Al-Kibar.

Both cases where cyber-attacks where employed show, although in different aspects, that a cyber-attack can be used to inflict costs on a target nation in a similar way as other coercive instruments.

The second criterion was that the instruments needed to apply to the coercive mechanisms specified by Byman and Waxman. By fitting the attacks into the political context and examining the effects of the attacks, it can be determined what mechanisms where employed. The findings of this study are shown below:

					Outcomes from the coercers viewpoint	
Coercer	**Target**	**Year**	**Coercers goals**	**Coercers key mechanism**	**Desired**	**Undesired**
Russia and/or Russian activist	Estonia	2007	Secure influence over the region, stop “derussification”	Weakening, unrest, power base erosion	NATO lost credibility in cyber defence	Estonia moved closer to NATO and EU, failed to stop the movement of the bronze statue.
Russia and/or Russian activist	Georgia	2008	Secure influence over the region	Weakening, Denial, unrest	NATO and EU negotiations stalled	Georgia reaffirmed its goals of Joining NATO and EU
Israel and/or USA	Syria	2007	Stop the proliferation of WMD	Denial, power base erosion	WMD program terminated	No overt undesired outcomes could be determined
Israel and/or USA	Iran	2010	Stop the proliferation of WMD	Denial	Costs on WMD program inflicted, WMD program delayed	Failed to stop enrichment program

In the case of Estonia there is clear evidence that the attack weakened the country as a whole and initiated, or at least facilitated unrest amongst the Russian minority. It can also be said that the attacks showed that NATO was incapable of protecting its member states from a similar attack, maybe prompting countries like Ukraine and Georgia to questions whether or not joining the alliance was a good move. In that case it can also be said that the attack was a form of power base erosion aimed against NATO.

The attacks on Georgia triggered similar mechanisms. It can be argued that weakening and powerbase erosion where employed in a similar way as in Estonia. In the case of Georgia, Russians also managed to deny Georgia political and military victory when they successfully thwarted their attempts to integrate the separatist regions South Ossetia and Abkhazia.

In the case of Iran and Syria the subsequent attacks could have been aimed to deny the respective target the continuation of their nuclear enrichment program. In the case of Syria the attacks may also have made North Korea more hesitant to cooperate, eliminating a key ally in Syria's attempt to acquire nuclear technology. In the case of Syria, the attack appears to have effectively ended the Syrian nuclear weapons program, but Iran has, so far, not shown signs that the attack has affected the regimes resolve to continue. The attack may have succeeded in delaying the program and has cast an uncomfortable light onto the Iranian program, but the nuclear proliferation was already under IAEA scrutiny as opposed to Syria, where the attack led to renewed interest from IAEA.

Both Estonia and Iran show evidence of cyber-attacks inflicting costs on the adversary, and doing so in such a way that the mechanisms of coercion where triggered, prompting some response from the political decision-makers. It is therefore possible to reach the conclusion that cyber-attacks fit the pattern determined by literature in order to be classed as instruments of coercive diplomacy.

How effective are cyber-attacks as coercive instruments?

The second question deals with the effectiveness of the instruments. There is some evidence to suggest that several of the criteria of coercive diplomacy suggested by George, where fulfilled when the coercer used cyber-attacks, as presented in a summary table below.

Notable, however, is the lack of apparent escalation or any clarity regarding the terms of settlement.

Clarity of the objective:

Clarity of objective, as defined by George, is imperative in order for the target to understand what is demanded. The targeted nation needs to understand what is demanded and how to act in order to avoid punishment.

In the case of Estonia, this is lacking. The Russian government and protestors conveyed demands varied from “don’t move the statue” to “don’t marginalize the Russian minority”. There are also varying theories for implied demands, challenging the NATO alliance sovereignty over the Baltic region (Herzog, 2011).

In the case of Georgia the clarity of the demands where similar, and Russia claimed to be acting to protect the lives of Russian citizens. As the conflict escalated the Russian demands where clear in that they demanded the withdrawal of Georgian forces from the separatist regions.

In the case of Iran and Syria, the overall objective was clear, the termination of the nuclear enrichment programs and/or nuclear weapons production.

Strength of motivation:

Strength of motivation determines how threating the attack is perceived. Without enough motivation from the coercing part, an issued threat is unlikely to be taken seriously. The coercing power needs to convey what it perceives as at stake and its preparedness to act in order to protect its interests.

All of the tested cases show considerable strength of motivation. The DDoS attacks where unprecedented in strength, coordinating thousands of hacktivists in the attacks. The Stuxnet worm was unprecedented in its complexity. The designers of the software had invested a lot of resources in order to make the program as potent as possible.

In the cases of Georgia and Syria, both Israel and Russia showed the targeted nations that they were prepared to use force in order to achieve their goals.

Asymmetry of motivation:

Asymmetry of motivation can be measured as the costs the coercing actor is willing to commit in relation to the costs the targeted nation is willing to undertake in order to resist the demands put forward.

In the case of Israel and Syria, or Israel and Iran, it is hard to determine the relative strength of motivation. The stakes might be perceived as higher by Israel than those perceived by Iran or Syria, if Israel regards a nuclear armed enemy as an existential threat and in the case of Syria, the Assad regime has made no further attempts to gain nuclear weapons, which may be a sign that the pressure from international actors combined with the displayed willingness and ability of Israel to target any installations, was enough for the Syrian regime to abandon its nuclear program.

In the case of Estonia or Georgia there is little to suggest that the asymmetry of motivation favours Russia. Both countries perceive Russian involvement in the respective crisis as attempt by Russia to meddle in their internal affairs and both countries perceive Russian interest in their respective countries to be an existential threat (Allison, 2008).

Sense of urgency:

The attacks on Estonia and Georgia clearly conveyed a sense of urgency for the political elite to act. Estonia, who prided itself of being a paperless society, suddenly ground to a halt, with politicians and security experts unable to thwart the attack, while Georgia faced imminent Russian invasion and military defeat.

In the case of Stuxnet, it is harder to discern a sense of urgency. It was probably stressful for the technicians and scientists working at the plant, having to suddenly deal with increased failures, but there are no indications that the political decision-makers where conveyed a sense of urgency.

That was also the case in Syria, where there were no signs that any other actions would follow the attack. It also took substantial time before details emerged enough for IAEA to inquire into the matter.

Adequate domestic and international support:

It is important to note, that adequate support does not mean total support. In all cases examined the necessary support was gathered or assumed before the attack.

In Estonia, the attacks where mainly perpetrated by hacktivist and non-state actors and the attacks where hailed as a fight against injustice and in Georgia, Russia demonstrated that it could act without the consent of the international community.

In the case of Stuxnet and Al-Kibar, Israel and the US appear to have acted in mutual agreement. In the case of Syria, while not directly involved, the US appeared to have given silent consent to Israel to act unilaterally.

Opponents' fear of unacceptable escalation:

Evidence of the opponent's fear of unacceptable escalation exists in Georgia, but there are no indications that neither Estonia nor Iran feared immediate escalation following the attacks. In the case of Georgia, the government felt pressured to agree to an armistice agreement with Russia, giving Russia far reaching freedom of action, most probable due to fear of unacceptable escalation.

In the case of Syria, there might have been fear of escalation, but this study has not found any accounts supporting that idea.

Clarity concerning the precise terms of settlement of the crisis:

One aspect of cyberwar is the lack of direct attribution of the attacks. Both studied cases retained plausible deniability and where therefore characterised by the lack of any direct communication of terms or demands. The only case examined, which included precise terms of settlement, is the case of Georgia. The cases of attacks on Estonia, Iran and Syria all are characterise by the lack of direct negotiations between the conflicting parties.

Comparing the cases of cyber-attacks against the criteria that George suggested, shows that at least some criteria can be regarded as fulfilled. The second method for testing effectiveness can show if cyber-attacks are more, equally or less effective than other instruments of coercion.

Summary:

	Estonia	**Georgia**	**Iran**	**Syria**
Clarity of objective	No	Yes	Yes	Yes
Strength of motivation	Yes	Yes	Yes	Yes
Asymmetry of motivation	No	No	Plausible	Yes
Sense of urgency	Yes	Yes	No	No
Adequate domestic and international support	Yes	Yes	Yes	Yes
Opponents fear of unacceptable escalation	No	Yes	No	Yes
Clarity concerning precise terms of settlement of the crisis	No	No	No	No

The findings (depicted above) show that cyber-attacks, in the selected cases, did not show evidence that a majority of the factors that George established for effective coercive diplomacy where fulfilled. Neither did comparing the cyber-attacks with similar cases where other coercive instruments where implemented show that cyber-attacks fulfilled at least the same or similar criterions.

This raises questions on why cyber-attacks would be favoured over other coercive instruments.

Conclusion - Why cyber-attacks?

While there is little doubt that cyber-attacks *can* be used as coercive instruments, this study finds no evidence that cyber-attacks are more *effective* instruments than other coercive instruments. The reason for the use of cyber-attacks must therefore be found in other constraints.

The Stuxnet attack and the attack on Al-Kibar share many similarities. Both attacks where perpetrated (to some degree) by Israel and the US and both aimed at denying other regimes in the Middle East the ability to obtain nuclear weapons.

In the case of Al-Kibar, the Syrian nuclear research program seems to have been halted, as opposed to what happened in Iran. As suggested in theory the effects of coercion might backfire prompting the targeted nation to defend its stance more furiously in light if the attack.

The case of Estonia and Georgia share many similarities: Both are countries that are former Soviet republics, both countries are in Europe and both countries have a large Russian-speaking minority. The difference is that Estonia is far more integrated into the European Union and NATO than Georgia.

Both conflicts where about the influence of Russia or Russian minorities in the country. Neither conflict seems to have affected the aim of the political elite to further integrate their respective country into both NATO and EU. In the case of Estonia, that work is already done and the cyber-attacks don’t seem to have affected political decision-making in any way favouring Russian interests. In the case of Georgia the country still is in the process of entering both the EU and NATO. It is, however, possible that the conflict was more successful in halting the process, as nearly six years have passed since the Bucharest summit, where Georgia, together with Ukraine, where declared likely future NATO members. Both the cyber-attacks and the Russian-Georgian war might have been intended, not against the attacked countries, but at a wider audience, warning countries perceived to be within the Russian sphere of interest, that there where consequences of distancing from Russia, which neither NATO nor the EU could protect them from (German, 2009).

Coercive diplomacy is a dynamic process and the end result of the studied cases may not be known for years to come. Similarly as with other diplomatic activities it will take years before any certain conclusions can be drawn about the long-term effects of the cyber-attacks on political decision-making.

Comparing cases involving coercive diplomacy in a methodically satisfying way is therefore problematic. There are simply too many factors to allow for isolation of the relevant factors. The results described in this study do not conclusively answer the question if cyber-attacks are more or less effective than other coercive instruments.

When comparing the cases, however, an interesting pattern can be discerned: both cases of the studied cyber-attacks, even though they show similarities to the cases where kinetic force was employed, exhibited significant disadvantages and high risks with a military action such as invasion, land grabs or air strikes. The lack of attribution, offering plausible deniability, limit the overt connection between a threat and action seems to limit the response to the attack.

Issuing a threat publicly puts pressure on a regime to respond to the threat to remain credible. A regime might find that the political cost of resisting the threat might be lesser than the cost of meeting the demands, causing a coercion to backfire and locking the target in its opposition.

In the case of the attack on Al-Kibar, major concerns lay in how Syria would retaliate and Israel undertook measures in order to minimise the risk and scope of a potential retaliation. Attacking Natanz with a cyber-weapon, sparked limited overt response from Iran. The initial lack of attribution made it hard for Iran to respond in the initial phase with force.

The same can be said for the case of Georgia and Estonia. Estonia is part of the NATO-alliance and enjoys the protection of article 5 of the NATO charter. A direct strike on Estonian soil as with Georgia would have forced other NATO partners to respond with force, an escalation Russia probably preferred to avoid.

NATO, which is trusted to shield Estonia from Russian invasion, however, could not hinder Russian hackers to attack over the internet. Similarly for the Stuxnet attack, many political analyst argue that Iran would have been compelled not to bend to the will of Israel and the US, but to counter-escalate with a military response should air strikes have been used. The Iranian safeguards which discouraged an air strike, had no impact on the risk of cyber-attacks on the country.

Suggestion for further studies

This study has shown that cyber-attacks can cause suffering and that suffering acts on similar mechanisms for coercive diplomacy previously established in literature, forcing political decision-makers to react. The findings further point to the plausibility that the constraints put in order to limit the use of force need not apply to the use of cyber-attacks. Further research is needed in order to conclusively determine this.

It is interesting to note that neither the cyber-attacks on Estonia nor on Iran have provoked any overtly violent response in the way that an armed attack would. Thus, NATO was quick to determine that the DDoS attacks on Estonia did not signify an armed assault in accordance with article 5 in the NATO charter, and did not oblige the allied countries to respond in the same way as if Estonia had been invaded.

Thomas Rid is right in his assumption that the indirect damage, which cyber weapons cause, limits the perception of a cyber-attack as an armed attack. While it is not possible to liken cyber-attacks directly with invasion, airstrikes or land grabs or any of the other suggested coercive instruments provided by Byman and Waxman, such attacks target the coercive mechanisms in their own unique way.

This study suggests that cyber-attacks work because they target different vulnerabilities than other coercive instruments. The lack of security in IT infrastructure exposes countries, which otherwise have protection enough to deter coercing attempts.

Reports warning of the dangers of cyber-attacks as political tools are plentiful, but the scientific study of the political use of cyber-attacks is limited and more descriptive research on the use of cyber-attacks for political reason needs to be done before any conclusions can be drawn.

Since cyber-attacks can be used as instruments for coercive diplomacy and the problem with attribution makes it hard to retaliate, cyber-attack might be an appealing instrument when military, or otherwise overt actions, are undesirable. Because the high cost-effectiveness, in that regard, one can expect to see more cyber-attacks used for coercive diplomacy in the future. Many nations invest in defensive and offensive cyber capabilities, and we are most likely to see increasing use of cyber-attacks in the wake of political conflict.

This study has found that other factors than those established by George matter when coercive strategy is determined. The factors established by George cannot determine what effective coercive diplomacy is, and George makes no attempt to call his list neither necessary nor complete in order to evaluate the effectiveness of coercive diplomacy. Better tools evaluating the effect of coercive diplomacy, taking into account the dynamic process of coercive diplomacy, need to be developed.

Cyberwar might, as Rid claimed, never happen, but that does not mean that cyber-attacks will not be a serious concern for national security.

Bibliography

Allison, R., 2008. "Russia resurgent? Moscows campaign to coerce Georgia to Peace." *International Affairs,* 84(6), pp. 1145-1171.

Alvehus, J., 2013. *Skriva uppsats med kvalitativ metod: en handbok.* Stockholm: Liber.

Arquilla, J., 2013. "Twenty years of cyberwar." *Journal of military Ethichs,* pp. 80-87.

Arquilla, J. & Ronfeldt, D., 1993. "Cyberwar is coming." *Comarative Strategy,* pp. 141-165.

Bahgat, G., 2006. "Nuclear Proliferation: The Islamic Republic of Iran." *Iranian Studies,* 39(3), pp. 307-327.

Betz, D. & Stevens, T., 2013. "Analogical reasoning and Cyber Security." *Security Dialogue,* 44(2), pp. 147-164.

Binoy, K., 2007. "Cyberwarfare warfare between Estonia and Russia." *Contemporary Review,* Issue 1686, pp. 288-293.

Byman, D. & Waxman, M., 2002. *The dynamics of Coersion.* Cambridge: Cambridge University Press.

Esaiasson, P., Gilljam, M., Oscarsson, H. & Wängnerud, L., 2012. *Metodpraktikan,* Stockholm: Nordstedts Juridik.

Falliere, N., Murchu, O. L. & Chien, E., 2011. *W32.Stuxnet Dossier,* : Symantec.

Follath, E. & Stark, H., 2009. "How Israel Destroyed Syria's Al Kibar Nuclear Reactor." *Der Speigel,* 11 February.

Garwood-Gowers, A., 2011. "Israel's airstrike on Syria's Al-Kibar facility: a test for the doctrine of pre-emptive self-defense?" *Journal of Conflict and Security Law,* 16(2), pp. 263-291.

George, A. L., 1997. *Forceful persuasion: coercive diplomacy as an alternative to war.* Washington D.C.: United States Institute of Peace Press..

German, T., 2009. "David and Goliath: Georgia and Russia's Coersive Diplomacy." *Defence Studies,* 9(2), pp. 224-241.

Herzog, S., 2011. "Revisiting the Estonican Cyber attacks: Digital threats and miltinationas responses." *Journal of Strategic Security,* 4(2), pp. 49-60.

Iacono, J., Brown, A. & Holtman, C., 2011. "The use of the Case Study Method in Theory Testing: The Example of Steel eMarketplaces." *The Electronic Journal of Business Research Methods,* 9(1), pp. 57-65.

IAEA, 2013. *Implementation of the NPT Safeguards Agreement in the Syrian Arab Republic,* Vienna: IAEA Board of Governors.

Joint Chiefs Of Staff, 2014. *Cyberspace Operations,* Washington: Joint Publication 3-12 (R).

Kreps, S. E. & Fuhrmann, M., 2011. "Attacking the Atom: Does Bombin Nuclear Facilities Affect Proliferation?" *Journal of Strategic Studies,* 34(2), pp. 161-187.

Langner, R., 2011. "Stuxnet: Dissecting a cyberwarfare weapon." *Security & Privacy, IEEE,* 9(3), pp. 49-51.

Langner, R., 2013. "Stuxnets secret twin." *Foreign Policy,* 19 november.

Liff, A. P., 2012. "Cyberwar: A new "absolute weapon"? The profileration of cyber warfare capabilities and interstate war." *Journal of strategic studies,* 35(3), pp. 401-428.

Liles, S., 2007. *Cyber warfare compared to fourth and fifth generation warfare as applied to the Internet.* Las Vegas, IEEE, pp. 1-3.

Makovsky, D., 2012. "The silent strike." *The New Yorker,* 17 September.

McElroy, D., 2008. "Uranium Found in Syria by UN Nuclear Inspectors." *Telegraph,,* 10 November.

McGraw, G., 2013. "Cyber war us inevitable (unless we build security in)." *Journal of strategic studies,* pp. 109-119.

Miles, M. & Huberman, A., 1994. *Qualitative data analysis: An expanded sourcebook.* Thousand Oaks: Sage.

Murchu, L. O., 2010. *Symantec.* [Online]
Available at: http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities
[Accessed 20 October 2014].

Puheloinen, A., 1999. *Russia's Geopolitical Interests in the Baltic Area.* Helsinki: National Defence Collage of Finnland.

Reed, D. J., 2008. "Beyond the War on Terror: Into the Fifth Generation of War and Conflict." *Studies in Conflict & Terrorism,* 31(8), pp. 684-722.

Rid, T., 2013. *Cyberwar will not take place.* London: Hurst.

Russian IT-Review, 2012. *Russia Rolls Out State Cyber Security Policy.* [Online]
Available at: http://eng.cnews.ru/news/top/indexEn.shtml?2012/07/12/496257
[Accessed 17 June 2014].

Rydqvist, J. & Zetterlund, K., 2008. *Consequences of military Actions Against Iran,* Stockholm: Försvasets Forsningsinstitut, FOI.

Schelling, C. T., 2008 [1966]. *Arms and influence.* New Haven, CT: Yale University Press.

Singer, P. & Friedman, A., 2014. *Cybersecurity and cyberwar : what everyone needs to know.* New York: Oxford University Press.

Squassoni, S., 2006. *Iran's Nuclear Program: Recent Developments,* Washington DC: Congressional Research.

Stone, J., 2013. cyberwar will take place. *journal of strategic studies,* 36(1), pp. 101-108.

Theorell, J. & Svensson, T., 2007. *Att fråga och att svara: samhällsvetenskaplig metod.* Stockholm: Liber.

Traynor, I., 2007. *Russia Accused of Unleashing Cyberwar to Disable Estonia.* [Online]
Available at: http://www.theguardian.com/world/2007/may/17/topstories3.russia
[Accessed 7 October 2014].

Wilson, C., 2008. *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress,* Washngton DC: Library of Congress, Congressional Research Service.

Zetter, K., 2011. *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.* [Online]
Available at: http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet.
[Accessed 17 July 2014].