HÁSKÓLI ÍSLANDS

Stjórnmálafræðideild

MA-ritgerð í alþjóðasamskiptum

Cyber-security and Critical Infrastructure Protection: The Case of Iceland.

Jón Kristinn Ragnarsson

Júní 2010

HÁSKÓLI ÍSLANDS

Stjórnmálafræðideild

MA-ritgerð í alþjóðasamskiptum

Cyber-security and Critical Infrastructure Protection: The Case of Iceland.

Jón Kristinn Ragnarsson

Júní 2010

Leiðbeinandi: Alyson Judith Kirtley Bailes

Nemandi: Jón Kristinn Ragnarsson

Kennitala: 100481-3249

Abstract

Most modern countries depend on computers to a certain degree. With higher dependence the risk involved increases, as a single system failure could make a serious dent in a state's infrastructure. Cyber-threats have become one of the best-known threats of the modern world, and can be divided into several categories ranging from those affecting the security of the individual to serious matters of state. They come in turn from state, private-sector and individual sources and have already led to several crises of international significance.

Iceland has long been proud to be in the forefront of many technological advances, and for instance the usage of computers in Iceland is among the highest in the world. But in the case of technological advances, security advances must follow or the whole state becomes vulnerable. In the modern world there are several options for a state that wants to improve its cyber-security, including chances to cooperate with various international agencies.

In this thesis Iceland is examined in terms of cyber-vulnerabilities relating especially to critical infrastructure. It will be asked what efforts Iceland has already made in this field but more importantly what efforts still need to be undertaken, drawing upon the opinions of several experts at different levels in both government and the private sector. Iceland has long been rather passive when it comes to international cooperation in security, and many reasons for this can be found including most recently the crisis now gripping the country. It can however be assumed that this crisis will one day pass over. The question is whether it will then be too late to start to look at security measures for the country. As will be revealed in this thesis, not all international measures need to require much funding, and international cooperation can be beneficial for all concerned.

Úrdráttur

Flest nútíma samfélög treysta á tölvur að einhverju leyti. Með auknu trausti sem lagt er á tölvur eykst áhættan, þar sem einstök kerfisbilun getur valdið alvarlegu áfalli fyrir innviði ríkis. Tölvu-ógnir hafa orðið ein þekktasta ógn hins nútíma heims og er hægt að skipta í nokkur stig allt frá vanda fyrir einstaklinga til vandamála sem ríki standa frammi fyrir. Þessar ógnir geta þá einnig komið frá ríkjum, einkageiranum og einstaklingum, og hafa þegar valdið stórum alþjóðlegum málum.

Ísland hefur lengi státað sig af því að vera framarlega þegar kemur að tæknilegum framförum, en tölvunotkun á Íslandi er til að mynda með því hæðsta í heimi. En þegar kemur að tæknilegum framförum þurfa öryggismál að vera samstíga, því annars gæti allt ríkið verið viðkvæmt. Í nútíma heimi eru nokkrir möguleikar fyrir ríki sem vill bæta tölvu-öryggi sitt, þar á meðal að vinna með mörgum alþjóðlegum stofnunum.

Í þessari ritgerð er tölvu-viðkvæmni Íslands skoðuð, og þá sérstaklega í samhengi grunninnviða. Það verður skoðað hvað Ísland hefur þegar gert til að bæta öryggi sitt en einnig hvað þarf að bæta. Það verður metið með ráðleggingum sérfræðinga frá ýmsum stigum samfélags, bæði úr opinbera- og einkageiranum. Ísland hefur lengi þótt frekar aðgerðalaust þegar kemur að alþjóðlegri samvinnu á öryggissviði. Margar ástæður er hægt að nefna því til afsökunar, meðal annars kreppan sem gengur yfir landið. Það er hins vegar hægt að reikna með því að sú kreppa muni einn daginn ganga yfir. Spurningin er hvort þá verði of seint að fara að líta til öryggismála fyrir landið. Eins og fram mun koma í þessari ritgerð þarf alþjóðleg samvinnu ekki ávallt að kosta mikið fjármagn, en hún getur hins vegar verið hagkvæm fyrir alla sem að koma.

Preface

When the topic of cyber-security was presented to me in the summer of 2009, it was very fitting for me. Having been interested in computers for a long time, I had also been fortunate enough to have worked in Iceland's infrastructure, first for Síminn and then for Fjarski (Landsvirkjun's communication department). I had seen at first hand several examples of just how vulnerable Icelandic infrastructure seems to be, and also noticed that there seem to be no real measures to counter this vulnerability. I had also noticed that while there might be several capable actors in Iceland, none of them seemed to be working together for the common interest of the Icelandic people.

In many ways this thesis combines many of my greatest interests. While computers and Icelandic infrastructure play a large part, there is also considerable focus on the international bodies that are looking into cyber-security, While in many cases the number of international organizations seem to make matters more difficult rather than easier, in the case of cyber-security the threats seems to be capably handled by all these actors, while still leaving a place for small states such as Iceland.

I would especially like to thank SI - the Federation of Icelandic Industries and the Institute of International Affairs - for a valuable grant in aid of my studies.

During the work on this thesis I have benefitted from great support from friends and family. I would especially like to thank Ágústa S. Guðjónsdóttir, and also Kristmundur Þór Ólafsson and Orri Jóhannsson, as without them this thesis would probably not have been written. The invaluable guidance of Alyson Bailes has also made this process possible, and without her this would still just be a good idea. All the people I have talked to in the course of my research also deserve immense thanks. The responsibility for the final outcome is of course always my own.

This thesis is the final assignment in the MA studies of International Relations at the University of Iceland. It accounts for 30 ECTS credits and the instructor was Alyson Bailes, Adjunct Lecturer at the University of Iceland.

Jón Kristinn Ragnarsson

Table of contents

1 Introduction

Many experts and international organizations, both foreign and domestic, agree that cyber-threats are one of the most pressing threats that the world of today faces. Every user of the Internet feels some aspect of the threats that are out there, although few probably understand the full extent of the threat. Iceland has been in the forefront of many technological advances in the last years or decades, and the use of the Internet is no exception; but it remains to be seen if Iceland is acting in a safe manner on the Internet, or that the Icelandic government is taking the precautions needed to stay safe. This is not just a question about the safety of the Internet user or the computers of the government. This is about the safety of the Icelandic people. If Icelandic infrastructure is threatened or damaged the effects could be greater than is imaginable. The smallness of the country causes more things to be inter-connected than in many other countries. The failure of one system can then cause a failure in another system through a domino effect, with end results beyond reach of the imagination. The threat is present, and in this thesis it will be asked whether Iceland is ready to face that threat. Our situation is in many ways different from what other countries encounter, with trans-boundary emergency networks that can help when one system malfunctions. In turn that also means that a system in another country could bring down the national network, so Iceland's island status can of course also be counted as a benefit.

The main questions I try to answer in this thesis are three, and could be stated as: *What are cyber-threats? Are they a threat to Iceland? And what can Iceland do to try to mitigate this threat?* General cyber-threats from criminal organizations and hackers are now well understood but the full extent of the threat could be surprising; and there is the further angle that states are to an added degree using cyber-threats and cyber-weapons in their regular arsenal, along with 'traditional' weapons. All these aspects will be examined in the thesis. The second

question might be thought to be self-answering, as Iceland is a part of the global world and cyber-threats are a global threat, thus bound to affect this country as well. In this thesis however I try to look more specifically at how far and in what ways cyber-threats and threats to critical infrastructure affect Iceland. Is Iceland more vulnerable than other countries and if true to what extent? In the third phase, international efforts to combat cyber-threats will be examined. If Iceland is assessed as needing assistance in the fight, we can hopefully find a safe haven on the international scene, or at least as close to a safe haven as can be achieved. On the other hand if Iceland is relatively safe from cyber-threats and threats to its critical infrastructure, we could also become valuable members of the international effort to combat cyber-threats, since many nations are struggling to come to grips with this pressing danger.

As can be expected, most of the general analysis in the thesis is drawn from previously published material. When it comes to Iceland the matters become more interesting. Ministries in Iceland have worked on the establishment of a computer response team, and have in the process questioned some experts about cyber-threats to Iceland, and possible responses. That report is summarized in this thesis, along with added results from personal interviews carried out with numerous experts and individuals in the Icelandic community. The information is then used to build a clear picture about Iceland and its exposure to cyber-threats and risks. The findings on possible solutions for Iceland are then supplemented with advice from individuals at international agencies as well as from domestic individuals. (All these interviews were conducted both face-to-face and, where necessary, by electronic communications.)

In structural terms the thesis starts by asking how the relevant international relations theory applies to the present challenge, and looking at some interesting approaches that are needed to stretch the realist approach for this purpose. Realism theory was written many years ago, long before the possibility of cyber-threats could even be imagined. Because of this it is necessary to enhance the term, for instance by looking at the relevance of deterrence in the case of cyber-weapons. Deterrence theory was made for nuclear weapons, and there may be quite different rules when it comes to cyber-weapons, not least since they are invisible. It can also be interesting to look at crimes committed in cyber-space or virtual worlds, which - as will be seen - have become an actual occurrence.

In the third chapter we will look at cyber-threats in general. This means looking at the threat all the way from the individual hacker, breaking into computers to either cause damage or claim bragging rights, through the international organized crime group using the revenue from computer hacking to fund more illegal activity. The last stage consists of threats from states that are more and more looking to cyber-warfare as the next stage in warfare. Cases where other states have suffered substantially from attacks of dubious origin will be examined in some detail for their possible relevance to Icelandic contingencies.

Chapter four revolves around Iceland. Some reports and threat assessments have already been made about Iceland that include the cyber-factor, and these will be summarized in this chapter. We will also look to what Iceland has done in the past to make itself safer against cyber-threats and where the official plans are going in the future. We will then look to international efforts that are going on to fight cyber-threats. Many international organizations are fighting this global threat, so if Iceland needs help it can probably be found in some of these agencies. If Iceland is well defended, the country can then perhaps raise its own profile to help others who face this threat. This will all be examined in chapter five. The thesis will then end with conclusions and a bibliography.

2 Theories used in this study

There are many theories in international relations that attempt to explain the actions of states and other actors in the international system. Theories are used both to explain what has gone before, and to try to predict what will happen next. Needless to say, theory is significantly better in explaining the past than predicting the future. One of the dominant theories in the field is realism, which views the state as the prime actor: but as it does not quite explain all the actions of the state, it has been necessary to supplement it by neo-realist theory. The case of cyber-security, where there are more actors than just the state, provides a good illustration of the need to stretch the normal theories a bit. In the case of cyber-threats there is a need to look at possible roles not only of the state but of international organizations and other non-state actors, all the way down to the individual, who can have a large impact in cyber-matters. An individual with resources can be extremely powerful when the weapons can be brought into play through the telephone lines. Cyber-weapons are for the most part invisible weapons, quite different from the traditional weaponry of states, and therefore there is an added need to look into how a state would design and convey the strength of its arsenal, when the arsenal cannot really be seen. These last-mentioned aspects are quite typical of the category of threats now called ‘asymmetrical’, all of which have a tendency to challenge realist strategy and to stretch its scope.

Furthermore, the cyber-threat is a new form of threat that falls into a category of threats that cannot be fought by each state, but much rather by a cooperation of many states. That could be counted as a point against realism theory, but when looked at more closely it can be seen that cooperation is allowed under the theory in certain situations, for instance when there is a case of relative gains to be made by one state over another. Lastly, the anarchy of the international system is a major factor in realism theory. In the case of cyber-threats, that anarchy is multiplied. When an individual can be as powerful as a state, and states can hide the origins of an attack, the rules are certainly different. When anybody

can be an attacker and anybody can be a victim, there is certainly a need for some sort of theory to attempt to predict the future.

The theoretical foundation of this thesis lies mostly in realism and neo-realism, but these theories alone are not quite sufficient to describe the world of today, with the added dangers that the modernized world has brought us. Section 2.3 of this chapter therefore examines among other things two alternative or additional frameworks of theory in which the problem of cyber-attack and challenge of ensuring cyber-security may be approached. The first is the calculation of 'risk': a discourse that has until recently been more typical of the private than the public sector, and which might for that very reason be helpful in defining cyber-challenges that arise for companies and individuals as much as for states. The second is the concept of 'securitization', which in a sense rises above the other theories in asking why an issue should be defined as a 'security' one in the first place - and what the pros and cons may be of having it so defined, by the actors holding power within a system, or in some other way.

2.1 Realism (and its limitations)

Realism as a theory in international relations is based on the nature of man as a primarily selfish and power seeking organism. Individuals are grouped into states, and these states act in a unitary way to pursue the interests of the nation, which for the most part are to amass power. These states exist in an anarchic international system, where there is no real hierarchical structure. With no supreme judge to manage the system the states are forced to rely solely on themselves. Their foremost tools are the balance of power and deterrence, which they use to try to keep the international system safe for them.

The realism theory has evolved through the ages, but some basic foundations can be traced all the way back to Thucydides and his *History of the Peloponnesian War*. There the state (Athens or Sparta) is the main actor and although other actors may enter the scene they are not important. Another basic concept that has been connected with Thucydides is that the state is seen as a single whole. Even though there might be different ideas and opinions within a state, it keeps a unified front. The third basic idea is that the actor or actors who decide the course of the state are believed to be rational beings, which arrive at

their conclusions by weighing the strengths and weaknesses of the available options. The fourth point is that a state is concerned with the matters of security. The state can have enemies that need to be kept at bay and their enemies can be either within or outside the state itself. The state increases its security by altering the infrastructural capacities, building its economy and making alliances with other states that could face similar adversaries or similar threats (Thucydides, 2004).

The fact that realism theory sees the nature of states as based on the nature of man is a noteworthy point that adds interesting facets to the theory. 600 years after Thucydides, St. Augustine added his own perceptions to the theory of realism. He stated that humanity was flawed, egoistic and selfish, but added that man became that way rather than being pre-disposed that way by his respective maker. He based the idea of the human 'fall' on a biblical explanation, and although that explanation was mostly rejected, realists for the most part agree about St. Augustine's view on human nature (Loriaux, 1992).

The way realism theory actually works can well be illustrated in the actions of the United States during the Cold War. There the US tried to contain the Soviet Union by preventing its expansion beyond its sphere of influence. US leaders also supported other states that would follow their side and tried to weaken the states that were considered their adversaries.

Even though realism encourages unity, the theory itself does not follow that advice. The most powerful re-interpretation of realism is neo-realism, put forth by Kenneth Waltz in *Theory of International Politics.* Waltz wanted the theory to better explain what had happened in international relations and predict to a better degree the general trends of the future. According to Waltz the most important aspect of international theory is the structure of the system. The things to watch are how the capacities are distributed among the states and the absence of an overarching authority. A state's position in the system is determined by its capabilities and the system constrains the actions of the states within it. The system determines the outcome, rather than the actions of the individual states (Waltz, 1979).

Neo-realists believe that the structure of the international system determines the balance of power. In the system the possibilities of international cooperation are slim. The question of relative gains is also an important one in terms of international cooperation, as states that feel insecure in some way must ask how the gains from the cooperation will be divided amongst the cooperating parties. In the neo-realist worldview the state is driven by the need to have more power than the other states, and therefore any gains that go to the other states instead of their own are looked at with scepticism.

Cheating is also a concern within the neo-realist view. Because of the importance of relative gains, states could try to cheat in order to increase these gains. Awareness of this is a further factor tending to decrease inter-state cooperation.

Despite the differences in these two variants of realism theory, there is a major proposition that unites them, namely that the state is a rational actor within an anarchic international environment. This is what distinguishes the realist school from other large international relations theories, and also adds an interesting aspect in terms of cyber-security (Mingst, 2004, pp. 65-71). In the case of cyber-threats, the individual and other non-state actors are very important, and when it comes to cyber-threats an individual can be equally as dangerous as a state. It will also be pointed out later in the thesis that some threats are of the nature that they can hardly be overcome without international cooperation, and cyber-threats are such threats.

According to realism, no authority exists above the state, which is a sovereign actor. The anarchy of the system constrains the actions of the actors in power within the states and affects the distribution of capabilities among the actors. Realism for the most part holds a state-centric view. The sovereignty of the state gives it the right to govern matters within its own borders and affect its people, economy, security and form of government (Mingst, 2004, p. 106). The realist theory sees the individual constrained by the system, just as the state is constrained. Individuals are not considered to have the freedom to be as important as the system or the state, according to the theory. The only way the individual could make a difference within the state is by altering national interests through

action in very large groups (Mingst, 2004, pp. 155-156). Here is revealed a certain limitation of the theory when it comes to cyber-security, as the field of cyber-security is mostly based on problems arising through commercial use and actions by individuals. On a list of possible cyber-offenders, states would not be high on the list, as individuals and other non-state actors have so far much more often been found responsible for cyber-attacks and cyber-offences than states have.

Although realists contend that the system is anarchic they are ready to make use of international law and organizations. That is not because compliance in itself is a good thing, but rather that it is in the state's self-interest to comply. Even though the system is anarchic, there are benefits to an ordered world, where expectations about state behavior can be managed. It is for instance in the state's interest that its territorial rights be respected, and so international treaties defining territorial rights are a good thing and should be observed. That does not mean however that the state would not be prepared in some way for the contract to be broken. In the same respect, large international organizations such as the United Nations are nothing without the states that incorporate them. Since these states act in their own self-interest, they can hardly be counted on to work for the benefit of the global good. Indeed, realists believe that the constituent states will cheat when the time comes to deliver on the promises of the organization (Mingst, 2004, pp. 191-192). Here we could take as an example Article 5 of the NATO treaty, which declares that an attack on one member of NATO would be considered an attack on all members (NATO, 1949). That promise of 'Collective Security' could be disputed when we look at two NATO countries, the US and Estonia. The day after the terrorist attacks of 9/11, NATO and its members invoked Article 5 to support the US in a war against a loosely defined term, terrorism. But when Estonia was attacked – by cyber-means inter alia - in 2007, the response was not as quick, and it could perhaps be said that the answer has yet to come. One of the deciding factors of realism is that nations tend to make alliances in order to try to increase their security, but realize that the alliances are short-term and should not really be counted on. This can perhaps be seen in Iceland's own experience in recent years, as some Icelanders would say that its traditional alliance has abandoned it, when the nations it considered its friends denied its requests for aid in its hour of need.

Although realist theory states that international cooperation is often lacking, there are examples to the contrary. Even though at times some countries would fight against the setting of rules on the use of certain weapons, i.e. the states that use those weapons, those same weapons can turn in their hands. In the case of cyber-weapons, the states that use those weapons would certainly resist any rule-setting on the use of these weapons or any international cooperation in countering them. But when it comes to viruses, spamming, and things like that, every nation is on the same level and would want to fight against that threat, even if considered small-scale as a security problem. The same is the case when for instance international terrorist organizations use the Internet to organize their global efforts. Every nation would certainly want to fight against that, as every nation could be a possible victim, either from these particular terrorists or the next ones. Every nation has an interest in the matter, and every nation could lose.

Realists maintain that there are two main approaches to manage insecurity. These two methods are the balancing of power and the act of deterrence. Deterrence theory is based on the assumption that war can be prevented by the threat of the use of force. The US offered a famous new twist on this idea with its justification of a pre-emptive strike in the 2002 National Security Strategy (The White House, 2002). Deterrence theory is based on four assumptions. The realist claim that decision makers are rational is in the forefront. The leaders of states want to avoid war if the cost is greater than the possible benefits, which is most often the case. A second assumption is that the existence of nuclear weapons makes the possible level of destruction too great for a state to risk a confrontation with a nuclear state. Thirdly is the assumption that war is never the only available option for rational decision makers. Deterrence is based on the states building up their arsenals so as to be considered a credible threat. The status of the arsenal must then be conveyed to the possible opponent. The knowledge that aggression will be harshly met will then have a considerable deterrence effect (Mingst, 2004, p. 227). In a way it could be said that alliance building falls into this same category.

The nuclear threat is of course a very strong deterrent, as no rational leader would attack a nuclear state with the knowledge that the attack could also cause the destruction of his own state. What complicates the matter is the question of

whether the leader of a state is indeed rational, and there is also the realist claim that states may try to cheat. If a state is in a position to bluff other states by claiming that it is in possession of nuclear weapons, would that state not attempt that bluff? For another state to 'call that bluff', the costs could be enormous (Mingst, 2004, pp. 227-228).

2.2 The stretching of realist theory

Further to this general description of the realism theory, there are more factors that need to be taken into consideration when it comes to the modern world, not least in terms of the cyber-threat. These factors will be looked at in the remainder of this chapter. First, normal *deterrence* theory is based on the nuclear threat, but when it comes to cyber-threats, the matter is quite different. It is relatively simple to count the nuclear warheads in a state's arsenal, but to define what a cyber-weapon is, let alone to calculate its power and numbers, is of a quite different order of difficulty. Because of the fast-moving nature of cyber-threats, both in their evolution and in action, knowing what and whom is to be deterred is also extremely difficult. The anarchic state of realism is magnified considerably because of the speed of the cyber-threat. Section 2.2.1 expands on these problems, but they also highlight the need to bring extra or different conceptual frameworks to bear as discussed in the later parts of the chapter.

2.2.1 The matter of deterrence in the case of cyber-security

Realist theory places high importance on the method of deterrence as a way to avoid war or to minimize insecurity. The theory is based on the Cold War nuclear era, where the huge destructive power of the nuclear bomb was supposed to keep the rational state leader from attacking a nuclear state. The matter is considerably more difficult in terms of cyber-threats, but there are still some similarities. Both nuclear- and cyber-attacks can be considered cross-border, are often very rapid and can both serve a tactical or strategic purpose. The biggest difference between the two is of course the destructive power of the nuclear bomb, although the destructive power of cyber-attacks has sometimes been said to be extensive. Nuclear weapons are often the weapons of last resort in an arsenal, thus a minimal attack is seldom answered with a nuclear response. Cyber-attacks on the other hand exist at the lower levels of daily occurrences. In the case of the 2009 Georgia – Russia dispute, cyber-attacks were the first kind of attacks. Sometimes

there can be several hundred small-scale cyber-attacks in one day. At the time of writing this, no country has denounced the use of cyber-weapons and attempts to criminalize or regulate them through international law are in their infancy, compared with the multitude of treaties on nuclear issues. Also, the difficulty in measuring the cyber-arsenal and possible damage caused makes deterrence very difficult in terms of cyber-threats.

Yet another difficulty in the matter of cyber-attacks is that the identity of the attacker can effectively be masked, so it is either not obvious who the attacker is, or it can even be made to look as though someone else has committed the attack. In terms of 'traditional nuclear attacks'[1] this is not the case. With cyber-attacks, the damage caused directly by the attack can be difficult to predict. The collateral damage can also hardly be calculated, but in the closely connected world of today, the collateral damage can be predicted to be both vast and cross-border. In terms of Iceland, even though Iceland was not the direct target, it could very well succumb to collateral damage in an attack on mainland Europe or the US.

The deterrence theory depends on the premise that the possible attacker knows about the defence measures available and understands that they will be used in the case of an attack. In the case of cyber-matters this can be difficult. Not only can it be difficult to convey the strength of a cyber-arsenal to the possible attacker, but the fact that in many cases the message needs to be conveyed to an unknown attacker makes the matter even more difficult. The anonymity of an attacker is also a factor in the asymmetry between sides. Some sides can be differently dependent on digital networks, and so in a tit-for-tat scenario, one side could lose more that the other. In the case of an anonymous attacker, he could possibly lose nothing because he is unknown and retaliation is not possible. The realist fear that states and individuals could cheat can also be taken into consideration at this stage. If a state can participate in warfare against another state without the risk of retaliation, there is a high risk that the state would attempt that warfare. Another factor in the matter of cyber-crimes is that if a state can fight another state, and not only use anonymity, but make it look as if another

[1] Not including loose nukes, for instance nukes in the hands of terrorist groups etc.

state is the aggressor, then that would be an even more tempting option. These are possibilities when it comes to cyber-crimes, as will for instance be seen in the case of cyber-warfare against Estonia in later chapters.

Although cyber-security has gained increased attention in recent years, there is still a shortage in understanding about the field. This deficit can causes problems when it comes to cyber-warfare. In the case of nuclear weapons there is an understanding on thresholds that should not be crossed and there are also international understandings about the definitions, categories, and possible uses of such weapons. This is not the case in cyber-matters, and that can cause threats to be misunderstood and instances of deterrence to go unnoticed. The collateral damage caused by nuclear weapons has for instance for the most part been calculated, and can be limited to an area around the place of impact. This is clearly not the case in terms of cyber-threats, although the full extent of possible 'fall-out' is hard to calculate.

The proliferation of nuclear weapons is of course a huge problem in the modern world. There are several international institutions that are spending vast resources on the subject, and are for the most part doing a good job. The proliferation of cyber-weapons is mostly going unnoticed, and since a simple Google search can provide some small scale cyber-weapons, these weapons are available to non-state actors as well as others. Groups and individuals come into the picture that are less likely than the rational state leader to be deterred by the promise of a retaliatory attack. With no territory, capital or infrastructure to protect, these individuals are more risk-prone than others and need not follow any rules that might be placed on state-action in cyber-space. This can then be added to the possibilities for masking the appearances of a cyber-attack so that it looks to be coming from somewhere else. There are extensive tools available to cover tracks in cyber-space, and these tools can be used in a military capacity.

In the nuclear age states could increase their arsenal to ensure a defensive effect. In the traditional context, more security as well as more deterrence would be gained with a bigger arsenal. This is not the case in terms of cyber-weapons. The capacities are by nature offensive, and with the difficulties regarding retaliation, it seems clear that that states should perhaps put more emphasis on

defence. The solutions to this new danger can vary from international regulations about the use of cyber-weapons to the setting up of national teams to defend against the threat. These solutions will be further discussed later in the thesis. Based on the evidence that has been stated here it could be said that cyber-threats are certainly a present threat, and because of the difficulty of assessing any state's relevant 'arsenal', their only way to know the size of another state's arsenal would by the possessor's own admission. But given the realist claim that states will try to cheat, this cannot be counted on. So the only thing that can rightly be known about the cyber-arsenal of states is that nothing can really be known.

2.3 Further frameworks for analysis

This section goes beyond realist and neo-realist theory to consider how newer theories and frames of reference developed since the end of the 20th century may help in the assessment of cyber-threats and -risks and in finding solutions. The first concept examined is that of asymmetrical threats, a term especially often applied to challenges from non-state actors since the terrorist attacks of 11 September 2001. Next is the application of risk analysis to public security, which again helps to build bridges between state and non-state security phenomena and the military and non-military dimensions. Crimes in a virtual world will also be briefly introduced and assessed in the light of the realism theory. Although virtual worlds are not something that the founders of the theory could have foreseen, they still provide quite a novel and interesting test of its validity. They may also illuminate important points when it comes to cyber-security, as real challenges for security arise for instance regarding the jurisdiction of a crime is when the crime is not really committed on this world, and the people connected with the crime could be separated by vast geographical distances. Finally this section looks at the 'securitization' concept which requires basic questions to be asked about what is a security issue, who defines it as such, and why.

2.3.1 Asymmetrical Threats

In later years there has been a huge discussion about the so-called 'asymmetrical threats'. These threats have been called asymmetrical because they allow a smaller, most often weaker, adversary to inflict damage on an often much larger enemy (Bailes, 2009). These new asymmetrical threats are often considered more trans-boundary than other older threats, and as is the nature with most trans-

boundary threats, are best fought on a trans-boundary level with cooperation among nations. They have also led to a widening of the focus of state security policy to include 'hard', high-priority threats other than traditional war. Terrorism and proliferation of weapons of mass destruction are most often cited as threats fitting into this category, but cyber-threats should justly be placed in this category. Although they can be seen as a form of terrorism they may also be used in other contexts (e.g. state against state and business against business) and deserve to be addressed separately. A good definition of an asymmetrical threat is that the user of the threat is often willing to use the weapon without the usual limitations imposed by the laws of war and mechanisms of deterrence, not least because he can hope to avoid meeting the attacked party in a direct force-to-force assault (Lambakis, Kiras, & Kolet, 2002, pp. 1). This explains why asymmetrical attacks are often considered to be especially ruthless in nature.

There are however problems with the definition of the 'asymmetrical' term, similar to those with the word 'terrorist.' These are subjective terms that change depending on whose point of view is used to define them. One man's terrorist is a freedom fighter to another and so on. What is an unusual threat for one individual is a standard procedure for another. Typical of the current, generally accepted discourse on 'asymmetry' is that the threats so described are novel and unusual from a Western perspective. The tools are often also unusual, and they are used against unusual targets, where there are often no international treaties about the use of the tool. The weapons used are often something that has a different function originally, but is used in a different way to cause harm. An obvious example is the 9/11 attacks, where airplanes were used as weapons. Difficulty in direct response is also a characteristic of an asymmetrical threat, including the fact that even responding with a large military force may be ineffective or counter-productive. Lastly, a significant characteristic is that the threats are indefinite and leave something to the imagination. For instance in the case of biological weapons, although it is well known that the results of such an attack will be extremely bad, the full extent is not known (Lambakis, Kiras, & Kolet, 2002, p. 13).

From these characteristics it is clear that cyber-threats should be considered an asymmetrical threat. Most of the characteristics set out above fit with them very well, although there could be some need for qualification in terms

of the relevance of a possible military response. As will be revealed in later chapters, several countries have already started building cyber-armies that can be used to fight cyber-wars. The fact that these wars would never be of the traditional sort could allow us to maintain that cyber-threat can be considered a prime example of an asymmetrical threat.

2.3.2 An alternative discourse: Risk

Risk is something that leaders of states and corporations alike need to take into considerations when planning for the future. Non-state actors have perhaps been the more usual users of the term, and the term has been used about these actors, but it is also important for leaders of states to take risk into consideration. In the modern world more risk factors have come into play, and more non-traditional responses have been needed. To understand this it is helpful to understand risk and to see by what factors it is governed. The modern world has also changed the nature of risk, and this can also be important to look at, especially in terms of cyber-security.

The idea of risk is embodied in the uncertainty over how the future in the very complicated world of today will unfold. Today's world is usually considered more complex and dynamic than before, which causes great fear of what the future may hold. But risk in itself is not a bad thing, as it can be divided in two parts, the potential threats that are included in the unknown, but also the opportunities that are linked with this risk. Because of this twofold nature, risk can be difficult to manage (Habegger, 2008, p. 13).

History has shown us that eliminating risk altogether would not be a good thing. It could be wondered where the human race would be if no one took risks. Eliminating every risk possible would also be extremely expensive without any real guarantee of success. The future would always bring what may come, without the possibility to be completely prepared for every contingency. The best possible way would be a middle way between threat and opportunity by use of risk analysis and management (Habegger, 2008, p. 14). This can to some extent be seen in the case of cyber-matters. Access to the Internet is considered common, but there are still some that want to limit that access, although the reasons behind that limitations could be questioned. Countries such as Russia and China have

been limiting their citizens' access, but that could be to protect the country and its elite, just as it could be to protect the citizens. It need hardly be mentioned that a complete closure is hardly ever a good idea, as a better alternative would be to manage the risk and funnel it into the correct tracks, where the risks can even be beneficial.

An undisputed definition of risk is very elusive, but there are three connected elements that are included in the risk landscape of today: interdependency, complexity and uncertainty. The constantly changing world amplifies all these elements. Advances in technology have increased the connections between states, institutions and individuals. The interdependencies have increased in correlation with these advances. International governance is no longer on a state-to-state basis and global actors are influencing political process on various levels of state governance. While some of these actors might have good intentions, there are of course some with malicious intentions. The technological advances have given them power and damaging effect hugely disproportional to their real significance (Habegger, 2008, p. 17). At the same time borders are quite insignificant for most non-military threats and risks, and because of the interconnectivity of actors the effects of events can spread rapidly and easily to other areas. Because of this it can be difficult to predict the consequences of an incident and also difficult to contain it within a geographical area (Habegger, 2008, p. 18).

Preventing a risk altogether is almost impossible. Total prevention requires total control over future developments and would always require immense resources, while – as noted – accepting the risk can also open up opportunities that would perhaps otherwise not be available. The aim of risk mitigation is thus not to completely eliminate every possible risk, but much rather to reach an adequate and justifiable degree of residual risk (Habegger, 2008, pp. 25-26). For instance it can be pointed that Estonians have in many ways put their main focus on the fight against cyber-threats. The main reason for that focus shift is perhaps because of the 2007 attack cyber-attack against them, but this has also made a convenient niche for the Estonians to place their emphasis.

Risk and threats are very similar terms that have no doubt at times been mixed together, but there is an important difference. The threat term has been used to describe problems that have been actively created by a security actor, and that actor can be anyone from a person to a state to any non-state actors (Bailes, 2007). So it is possible to refer to cyber-threats as they are posed by actors in the system, whether those actors are states or individuals. Risks are somewhat different. The nature of risks is to be in large part reflexive (Bailes, 2007). That is, it is the decisions of humans to live as they do, to perform the activities that they do and to travel to the places that they travel to that in fact makes them vulnerable. It is the willingness to live in an open community that makes access by criminals easier. It is the technological advances that are introduced to make life easier that often bring with them new risks that have to be weighed as acceptable or unacceptable compared to the possible benefits. And just as in financial matters, the highest benefits often come with the greatest risks. In this closely connected modern world it is also highly likely that someone actually endures the risks without any real gain. For instance it could be said that although all the Schengen states share the risks of their common area of free movement, the benefits are more for some states that for others. An open country is beneficial for someone who wants to be able to leave with ease, but is perhaps not beneficial for the ones that are left behind. Another example could be that a state is willing to work with uranium as it is considered in the best interest of the state, but the citizen who endures the radiation risk does not really have a say in the matter.

The current risk landscape is made even more intense by a few specific characteristics of systemic risk. Firstly they are often marked by a slow rather that quick evolution, meaning that the presence of a particular risk might not be apparent at early stages. Contingency plans can obviously not be made for completely unknown threats, but this slow evolution can also cause isolated problems to be fixed rather than the complete system being looked at. Secondly, the spread of a systemic risk is often gradual and the actual consequences might not be apparent before it is too late to be fixed. Thirdly, if two systemic risks eventuate at the same time but in a different sub-system or at different geographical locations, the effects can be amplified and the appropriate counter-measures might not work. Such simultaneous occurrences can cause effects that

are completely unforeseen and in effect cause an evolution of the systemic risk, causing much more extensive damage (Habegger, 2008, pp. 18-19). Thus increased complexity leads to a higher degree of uncertainty, and one of the main challenges both for international business and state politics is to detect the future trends through the uncertainty. As already noted, the new capacities and uncertainties added by modern technology reinforce the realist thesis about the anarchic international system. It can then be said that because of the technological advances of the modern world, the system has reached a state that could be called extreme anarchy. If traditional realism says that in a state of anarchy suspicion is high, it can be said that suspicion is even higher in this new extremely anarchic international system.

Modern technological advances may of course also be viewed more positively, as transforming existing crimes rather than producing new ones, and as providing extra tools for detection and response. An excellent example of this is organized crime. One of the world's oldest professions has seized upon the advances in communication technology and evolved immensely. Because of the added attention that cyber-crimes have received in recent years, it would be easy to assume that those were additional crimes, on top of the crimes already committed. But the case seems rather to be that the crimes committed through the Internet are actually rather the old crimes in a new costume (Nisbet, 2003). Attempts to scam unsuspecting people of their money through an elaborate scheme are not a new thing, though it has probably not been done on such a large scale as in these recent years. But the same advances have also provided new tools to fight these older threats. International law enforcement agencies are now working within a trans-boundary network where a suspect can be found in a different country or a different continent, with information sharing in real-time. Information on new threats can also help states prepare for the oncoming threats, and together these countries and agencies can help to eradicate them. Faster communications shorten innovation cycles and can provide increased opportunities (Habegger, 2008, p. 19).

Possible risks need to be categorized by the classical definition of risk as the product of damage potential and the likelihood of occurrence. There are two fundamental mitigation strategies that can be distinguished: preventative measures

and precautionary measures. Preventative measures are intended to prevent the occurrence of the event and are because of that directed at the cause of the particular risk. Precautionary measures are intended to alleviate the damage that might be caused by the occurrence, and are therefore aimed at reducing the vulnerabilities of an institution or society (Habegger, 2008, p. 25). This challenge has recently been addressed for the first time across a comprehensive range of threats and risks in the case of Iceland (Foreign Ministry of Iceland, 2009[2]). The Threat Assessment report published in 2009 categorized the possible threats against the country, and pointed out what needed to be done in the fields where improvements were needed. The Threat Assessment will be better described in later chapters when the focus will be put more firmly on Iceland.

But why is risk a useful concept to apply in terms of cyber-security? As explained in this section, risk is reflexive, and the more an actor depends on something, the more risk is created because of that dependency. There is hardly a state in the world that has not transferred some of its dependency to computer-based networks, to different degrees. As citizens have gotten used to the comfort that this can bring, no one is willing to go backwards. Businesses are looking to cut cost as possible, especially in a recession, and one way to cut costs is often to switch the human hand for a computer. Military actions – ranging from intelligence gathering, surveillance and early warning to battlefield systems - are getting more and more computerized, and in the close future we could perhaps even see a war fought without any human losses. All these things point to the fact that the modern world is extremely dependant on computers and cyber-systems: and the risk that follows this dependency cannot be eradicated, only managed and responded to.

To know how to manage the risk, the first steps must surely be to map the critical infrastructure of a state and to find where the weak points are, in terms of vulnerability to attacks but also human error or malfunction. Critical Infrastructure is the name of the most essential structures and services for the functioning of a state and society. This could for instance be water, electricity,

[2] Threat Assessment for Iceland. The report is available at http://www.utanrikisraduneyti.is/media/Skyrslur/Skyrsla_um_ahattumat_fyrir_Island_a.pdf English part is at the end of the report.

communications, and so on. Transportation could also be fitted into this category. The needs and possible methods of Critical Infrastructure Protection will be looked at later in the thesis, both in terms of Iceland and Europe. In many cases, and especially in realist terms, the first step when critical infrastructure is damaged would be to look for the attacker and counter-attack. But in the case of Iceland, this would not be the case as the most important task would be to manage the damage – which throws the emphasis back on mapping and reducing vulnerabilities. When the attacker could even be un-findable, it is definitely better to work on the minimizing of risk rather than some aspect of defence that would not even necessarily work against the threat. When a state is attacked or if any of the vulnerable sectors become unworkable, modern society is so inter-connected that every aspect of life across the community could feel the effect. Because of this there can hardly be a reason for a separation between private and public sector when it comes to minimizing the risks, and it is of course in the interests of the private sector to have as little risk as possible.

2.3.3 Virtual crimes

Crime has begun to fester. Organized crime groups, such as mafias and gangs have begun to take over places and make them their own. Mobs run free. Shopkeepers are closing their shops for fear of being victims of theft. The citizens look to the president for guidance but he has none to offer. He wants the people to take care of the problem themselves.

Although these stories could very well be from the real world, these are tales of people from the online virtual community Second Life (Holahan, 2006). Second Life has more than a million members, who carry out transactions in their own currency, the Linden. The Linden has been pegged to the American dollar and can be traded openly. Second Life is a digital community where members of the community interact, purchase and sell goods and build property that is worth real-world money. The community even has architects who design houses and buildings for the other members of the community, and clothing stores with original designs made by the owners of the shops (Holahan, 2006).

And like any other community, Second Life faces crime. There have been computer viruses and cheats that make it possible to copy an artefact inside the

game. This means that a thief can go into Second Life and copy an item without paying for it. That item could then either be owned or sold by the thief. If it were sold, the prize can be counted in actual real-world money, and this is where the matter gets difficult. If the stolen item were only sold for in-game money that has no real worth in the outside world, the matter would then normally be handled in-game, by the members of the community or by the makers of the game. But because of the trans-boundary nature of the crimes, the makers of the game have been unwilling to take on the role of police and judge. They have been willing to ban anyone who has been caught stealing, but that by itself does not cover the financial damages that may have been caused by the crime. The makers have also been working on crime prevention, so that it is known whether an item has been illegally copied, so that the community itself will either shun the offender or that he will by sued by the original designers. That court case could either take place in the real world or in a Second Life court system (Holahan, 2006). Here it is normal to ask, where should the jurisdiction lie? Should it follow the perpetrator, the victim or the place of the crime? These could be three different places, and in the case of the place of the crime, it is not a real actual place, but a virtual one. These are problems that need to be solved.

The members of the Second Life community have been pushing for a sort of vigilante justice. Members have set up associations to weed out bad players, and public lists of cheaters are published. But just as in any other case of vigilante justice, there are risks and questions that need to be answered. On what authority do these vigilantes act? What punishment can they deal out? Who do they respond to in the case of a mistake? If a member or shopkeeper is falsely accused and blacklisted, who do these individuals complain to get possible damages (Holahan, 2006)? It should be noted that these are all questions that could be asked in the real-world if a similar situation were to arise. This again points to the conclusion that security problems and criminal issues arising in a virtual or cyber environment are very similar to the affairs of the real world, but simply come in different packages.

At first glance one would think that a virtual world such as Second Life would fall outside the realm of realist theory. But when looked at closer it becomes clear that the actions of people in the virtual world are no different than

those of the real world, as people seem to act on the same impulses. The main difference could be in the repercussions of these actions. The similarities of the two worlds go on: the authorities of Second Life have been unwilling to take on the role of law enforcement in the community, instead opting for a vigilante-type justice. When the normal authorities of a state do not address a threat such as cyber-threats, they actually leave it in the hands of the citizens or businesses to take care of the threat and defend themselves. Although for now the actions of these cyber-vigilantes could be considered mild and mainly focused on defence, it could perhaps not be far until a pre-emptive justice would be considered more feasible. Cooperation without a middle agent such as a state can be very fragile. Even when there is a middle agent that agent needs to be respected or the cooperation could fall apart when the players see something better or believe that their interests are better served on the outside. Examples of this can be seen in the real world, where the United Nations can work as a middle agent of sorts, but when the interests of the states lies outside the UN states can be quick to go their own way.

The similarities between the real world and the virtual world are extensive, and the virtual world seems to be sharing in both the benefits and drawbacks of the real world. The full extent of this similarity is hard to predict, but the benefits are already extensive. Virtual worlds have been used to predict the spreads of diseases on a global scale. At first there were some troubles with the anomalies, but with better virtual worlds the anomalies have been calculated into the worlds (Epstein, 2009). For instance there is the Global-Scale Agent Model (GSAM) which has approximately 6.5 billion distinct agents, who move and interact just as realistically as the available data on the real world allow. If this virtual world can predict the actions of people with some accuracy, that could perhaps be used for other valuable purposes, and even be used to predict the actions of states. The final piece of a full circle move would perhaps be a virtual simulation of a state response to a cyber-threat. That situation is not outside the realm of possibility in this modern world of ours. The only limits of use for the model simulations are probably just in the mind of the inventors, so these simulations could perhaps someday be used to track the proliferation of WMD and so on. There certainly are many interesting possibilities to consider.

2.3.4 Securitization

Because of the nature of cyber-crime, it has been potentially an issue for state, business, and personal security from the beginning. But if a state were to deliberately down-play and minimize the threat from a certain danger, for instance the danger of cyber-crime, could it be said that the matter has been de-securitized? The way that the profile of cyber-crimes as a significant threat has been boosted by media and public debate in recent years makes it worthwhile to look at the concept, and the modern reality, of 'securitization'. Firstly the term itself will be explained and some implications reviewed, then cyber-security will be looked at through the securitization lens to see what the status is in that regard.

The concept of securitization is usually connected with the so called Copenhagen school of international relations, and revolves around how the 'security' term is viewed and used in the public discourse. The act of securitization involves using the term 'security' about a specific field or matter, and thereby making that particular matter more important. Classic analysis of securitization claims it as a method for states and institutions to use as a way to assert control over the issue or field concerned (Wæver, 1995, pp. 54-57). The question of who performs the securitization will be looked at later in the section.

The security framing of a matter makes it something for the security elite to handle, possibly away from the public eye. It is then at the elite's discretion to decide whether something is a security problem. The leverage created by the connection to security can be very powerful, as security matters are often considered the foundation of other politics. Economic, social and other goals can never be pursued if there is a constant threat to survival (Eriksson & Giacomello, 2006, p. 11). As such the security term is heavily loaded, and threats to security would most often be answered with greater haste, gravity and force than most other matters (Eriksson and Giacomello, 2006, p. 11). Security definitions and norms can also be used to stop political change, mobilize the population in certain direction, or allow resort to extraordinary means (Wæver, 1995, pp. 54-57).

Just as an act of securitization puts an issue in the forefront of public policy, there is an opposite. The act of de-securitization can be used to remove an issue from the security sphere. That would reduce the attention the matter would

receive, and also militate against the use of secrecy and other measures that could follow in the case of high matters of state. This does not necessarily mean that an issue is not important, but rather means that the issue can be the object of a democratic decision process rather than being handled by 'experts' and in haste, as is often the case in security matters (Eriksson and Giacomello, 2006, p. 11).

A definition of a security problem according to Ole Wæver is something that threatens the sovereignty of a state in a particularly urgent or dramatic fashion. The threat can also weigh on the state's independence and limit its capacity to handle its own affairs. This sort of threat would have to be met with the mobilization of maximum efforts (Wæver, 1995, p. 72). The key terms of this definition, urgency and the risk of undermining state capacity are highly representative of cyber-threats. They are certainly very quick acting, and are often very dramatic. Any serious cyber-attack would certainly aim at disrupting a state's critical infrastructure and therefore limiting the state's capacity to act. Accordingly, the cyber-threat should be met with the mobilization of maximum efforts: but what the relevant resources and actions would be in the case of cyber-threats could perhaps be difficult to say.

Military threats have for the most part been in the forefront of the security literature. This is, according to Ole Wæver, because of the swiftness with which the threat emerges and because of the power of the threat. If a state was defeated it would be laid bare to the will of the conqueror (Wæver, 1995, p. 71). There are some similarities here to the cyber-threat; mainly the swiftness with which the threat emerges, but also the fact that a successful cyber-attack could leave a state completely without control, totally under the will of the conqueror, whoever that might be. Because of these similarities it can certainly, at a minimum, be said that cyber-threats are viable as security threats and should be taken seriously. Indeed it could be said that cyber-threats are quickly becoming the greatest threats of today. This is because that although cyber-threats are similar to military threats in many ways, they also go beyond them in many respects, for instance in the trans-border aspect and the fact that often it can be quite difficult to prove guilt in the case of cyber-attacks.

The literature depicts security as freedom from threats, both objectively and subjectively (Wæver, 1995, p. 71). In the case of cyber-threats there can never really be a secure moment according to this definition. Although states may keep the peace, the non-state actors need not follow any treaties or codes. That is yet another reason why cyber-threats could quite justly be called the greatest threat to the world today.

2.3.4.1 Who performs the act of securitization?

The question of who performs the act of securitization is an important one. Ole Wæver talks of the elite, who would use the act of securitization to make a matter more important (Wæver, 1995, p. 73). He also talks of the 'state-representative' who may utter the word 'security' and move an issue into a specific area of governance, making it subject to special rules so that any means necessary are allowed (Wæver, 1995, p. 73). There are in a sense no limits to what a state might do to protect itself from such a threat, and there are obviously great powers for the power-holder in the case of securitization (Wæver, 1995, p.74). The danger of selfish use of the power of securitization by the power-holder can be hard to avoid, according to Wæver (Wæver, 1995, p.73).

Regarding who performs the speech act, it should be asked if other actors should have the power to securitize. For instance, it could be asked if the media should have the power. The EU's Eurobarometer survey regularly carries out studies on security concerns of the people of the member states. The responses of the people mostly reflect the softer aspects of security, rather than the harder military aspects. Perhaps the publication of such a report could be called an act of securitization (Ólafsson, 2009, p. 20). Wæver argues that giving the power of securitization to non-state actors could be troublesome. It could lead to racism and xenophobia, or even the securitization of even more personal matters (Wæver, 1995, p. 82). But are the elite/power-holders/state representatives then necessarily the most capable actors for the securitization act? Wæver worries about selfish interests that could lead to the wrong things being made dangerous, but these same risks follow when the power is given to non-state actors, and there we also have the added danger of conflict of interests due to financial reasons. No one can be trusted completely, especially not according to the claim of realism theory that everyone is likely to cheat to further their own gains. But another realist claim is

that state leaders are rational actors, and that is why the power of securitization should be in the hands of the elite.

In the case of cyber-threats, there are several ways of judging the origin and correctness of securitization of the threat. It may be natural for the actors who are actively fighting the threat to put it in the public sphere of attention. But if these actors have a financial gain to make from the securitization of the threat, then things might be looked at with some skepticism. For instance, the private firms Symantec and McAfee provide reports on the cyber-threat, and often describe it as great. But given the fact that both these companies are in the business of selling security against cyber-threats, can they really be considered reliable? The most capable actor to perform the act of securitization would possible be a CERT-team[3] or something similar, but setting up such a team to start with would depend on a judgment that the cyber-threat was a real viable threat.

In fact, the situation is even more complicated because an issue does not need to be on the political stage to be applicable for securitization. There also does not need to be a real existential threat for a threat to become a security matter. A case needs simply to be successfully presented, with the correct vocabulary designed to get a public response, for an issue to be securitized; and in this sense there can be a large spectrum of possible 'securitizers' (Dunn-Cavelty, 2007, p. 22) – including the media as discussed in the next section. The framing of an issue can explain who is responsible and offer solutions, conveyed for example by images and metaphors. When the national security dimension is not obvious, specific analogies are often needed (Dunn-Cavelty, 2007, p. 23). This is a method that has become popular in recent years, where a new threat is compared to an older threat to provide a reference frame (the very notion of a 'war' on terrorism is an example). Of course the difficulty with this is that the new threat is often only comparable with the older threat because it is said to be so, and the analogy may particularly fall down when it comes to remedies.

[3] CERT-Team is a Computer Emergency Response Team. These have been set up by nations but also by smaller groups, such as universities. These will be discussed further later in the thesis.

2.3.4.2 Securitization by the media

As is probably the case with most possible threats, the cyber-threat can be consciously fabricated. It is even possible to find a rather simple guide on how to write a newspaper article that would cast the cyber-threat as the greatest threat in the world, at least for whoever does not have all the facts (Morozov, 2009). The first step is to give the article a catchy title providing an analogy to an older threat. An example would be 'Digital Pearl Harbor' or 'Cyber-Katrina.' The article should most likely begin with Estonia's story and also talk at some point about how the organized crime units have begun to use the Internet as their main field of operations. There should be many references to Russian and Chinese cyber-warriors. People with a conflict of interests should be given ample room to talk of the threat, and they should all try to sell their products that conveniently are used to fight cyber-threats. There should be mentions of the cyber-war between Israel and Palestine, but that should be called e-Palestine, as a nation in cyber-exile. Finally it should be mentioned that most US defence installations have been cyber-attacked a gazillion times, mention that Obama will fail his task at battling the cyber-threat and that Al-Qaeda recruits its members through the Internet (Morozov, 2009).

Although these examples are cited from an article expressing cynicism about 'cyber-hype', there are a few good points in there. Firstly it should be said that it would be difficult to write any article about cyber-threats without mentioning all these aspects, and as previously stated, any threat could probably be put in a dubious light with the right framing. And as this article satirizes the obvious ways of securitizing an issue, it actually makes a good job of de-securitizing the matter instead.

It could also be interesting to think about who or what can in fact work as a securitizer. Pop–culture can have an impact on how we see the world, and that can in turn affect attitudes to security. For instance in the case of cyber-threats, if a big Hollywood movie were to be produced where the main villain uses cyber-crimes as his method of choice, that can have an influence on the way common people see the threat. It could lift the threat to the status of a security matter, and that in turn could have an effect on the elite.

Securitization is an important factor in security studies. In the case of cyber-threats the question is who should be responsible for the task of securitization. Should it be the private sector that actually work with the danger, but could stand to make financial gain from the securitization of the field? Or should it rather be the elite, the people who have often been elected to take care of exactly these matters for their constituency? Even the elite are not above suspicion, but in the end they have to be counted to perform their respective jobs. The chapter shows that securitization can be manipulated by those that do in fact not have the power of securitization. This can certainly be considered a real danger, but in the end this danger will possibly always be present, and needs to be taken into account rather than only criticized.

2.4 Conclusions

In this chapter the realism theory has been described, as well as neo-realism. Realism theory states that the basic responsibilities of the elite should be to protect its citizens against any threat that might occur, including cyber-attack, whether that threat comes from outside or inside the nation. The state will use international cooperation as it sees to provide the most relative gains, all the while keeping other nations at arm's length for fear of cheating. The state will try to signal the power of its arsenal when available, for deterrence purposes, but when it comes to cyber-weapons, there can certainly be some trouble in how to convey the real might of both cyber-weapons and cyber-defences. This is one of several reasons for concluding that a realist analysis in itself is not enough. The notions of asymmetrical threat and of 'risk' as a denominator in security are both helpful in understanding the nature of cyber-threats and the conditions for successful response more clearly.

Modern societies have placed so much of their dependency on infrastructure, which is now in turn heavily dependent on cyber-systems that if damaged could cripple the state itself and all kinds of legitimate non-state actors. This damage can be because of an attack but can also be caused by man-made error or malfunction, but either way the possible risk and damage needs to be mapped so that it can be prevented or, at worst, limited and quickly restored. This mapping should be done in cooperation between private and public sectors, as

every actor within in the state is vulnerable because of the close interconnectivity of the modern society.

Virtual worlds are something that could hardly have been foreseen a few years ago, but are now an important aspect of thousands of lives. Looking at virtual worlds raises relevant questions that need to be answered in the coming years, because the influence of virtual worlds is surely going to increase in all fields including that of security. Finally, securitization shows us that security language certainly has power and that cyber-threats have gotten increased attention in recent years. Important questions on the matter revolve around who has placed that added attention on cyber-threats, and raise the questions of whether that agent was the right agent for that particular job. If the wrong agent has the power of securitization, danger can follow from the securitization of fields that should not be considered security matters, or from special interests that lead to a focus on inappropriate solutions.

In light of all this it would seem that cyber-threats are a viable and rising threat that could in the near future become one of the greatest threats the world has seen. Although the destructive force of cyber-weapons does not compare to that of the nuclear bomb, cyber-weapons go further than nuclear weapons in many ways and are superior to some extent, for instance in the fact that a huge cyber-arsenal can be kept on an item that is no larger than a coin.

3 Cyber-Threats in general

Becoming a cyber-criminal is not a very difficult task. A simple Google search for 'hacking tools' can provide you with several thousand good results, and with that you are on your way.[4] As experience increases so do the severity of the attacks, and before long you can be attacking the sites of official departments or hacking into command centres for critical infrastructure. All that is required is a computer, Internet access, and a little patience. When the economy is in a recession people seem to look more to the Internet, to search for job openings and bargains: criminal activity follows the people on to the Internet, and so cyber-crimes rise. When people are scared cyber-criminals can also use that fear to make money, selling people 'protection' that does more harm than good - a further impact of the Internet on real-life security.

In 2002, Richard Clarke, the then Special Advisor to the US President for Cyberspace Security, gave a briefing on whether the US was ready for a cyber-terror attack. He described the cyber-terror spectrum as ranging from the fourteen-year-old kid who hacks for the fun of it with no political or financial agenda, to the nation-state using cyber-weapons to perform espionage and/or subvert or attack other states. But that fourteen-year-old can be just as dangerous as other actors, and young hackers have for instance hacked controls for dams and airport controls in the US. Terrorist groups like Hamas, Hezbollah and Al Qaida have also been known to use cyber-weapons, for purposes that were not fully known in 2002 and can hardly be said to be fully known even today. All these actors will be looked at in further detail in this chapter, with specific international examples to show both the damage that can be caused in target nations and the kind of states who may be doing the attacking. The conclusion of Clarke's 2002 briefing – namely that the best way to defend against this threat was a joint effort from both public and private actors, with trust and information working both ways (Clarke,

[4] In this thesis the term 'viruses' is most often used. The term is used to cover malware and other man-made malfeasances.

2002[5]) – will be examined later in the thesis, with reference to how Iceland should fight the cyber-threat.

Chatham House, the home of the Royal Institute of International Affairs in the UK, has divided cyber-threats into four categories: state-sponsored cyber-attacks, ideological and political extremism, serious and organized crimes, and lower-level or individual crimes. This is a good categorization, and will be followed in the rest of this section. Under the headings of state-sponsored attacks, and of serious and organized crime, longer discussions are included on the problematic concept of 'cyber-war' and on the notorious example of the Russia Business Network (RBN) – respectively. Under the heading of low-level crime full details are provided of the most common varieties of on-line fraud against individuals.

3.1.1 State-sponsored cyber-attacks

As early as in September 2000, Israeli cyber-soldiers hacked into websites owned by Hezbollah and the Palestinian National Authority. The Palestinians responded with cyber-attacks on governmental and financial websites, calling it a 'cyber holy-war' (Cornish, Hughes, & Livingstone, 2009, pp. 3-4[6]). Another example often mentioned in terms of state-sponsored cyber-attacks is the assaults on Estonia in 2007. That particular incident will be examined in great detail later in this chapter, but it should be mentioned that while responsibility has never been proven there is high suspicion that Russia was behind the attacks. Again in September 2007, an Israeli military attack on Syria was assisted by a parallel cyber-attack which minimized the chance of detection. The parallel use of cyber-weapons with 'traditional' military weapons will be brought up again in the case of the attacks on Georgia in August 2008. As to the future, it is widely reported that China is looking into cyber-warfare, and that 'cyber-dominance' might be deployed as an early stage of Chinese war strategy (Cornish, Hughes, & Livingstone, 2009, pp. 4-5). China will be looked at further later in the chapter.

To understand the appeal of cyber-weapons for attacking a rival state: it has been estimated that a large-scale DDOS-attack (Distributed Denial of Service,

[5] Report available at www.estrategy.gov/documents/cyberterrorattack.doc
[6] Report is available at http://www.chathamhouse.org.uk/publications/papers/download/-/id/726/file/13679_r0309cyberspace.pdf

explained later in this chapter) on the US could for instance have devastating effects. If electronic communications could be kept offline for three months the damage has been estimated to be similar to 40-50 large hurricanes striking at once (Cornish, Hughes, & Livingstone, 2009, p. 4).

3.1.1.1 Cyber-crimes or Cyber-War?

The computer company McAfee publishes a Virtual Criminology Report on a rather regular basis, and in the 2009 report they named four key attributes for a cyber-attack to be able to be classified as an act of cyber-war.[7] These four attributes were then compared with the latest cyber-attacks to estimate the severity of these attacks. While the term cyber-war is now so often bandied about that it was a useful idea to try to clarify it, the key attack attributes suggested by McAfee are themselves open to question. They are:

1. Source: Was the attack carried out or supported by a nation-state?

This criterion may be challenged since non-state actors – including large terrorist networks - today have significant security roles and power even when not backed and exploited by a state. Considering the prevalence of internal conflicts today, to claim that only a state can participate in war is a peculiar statement. Conversely, the US has declared since 2001 that it is fighting a 'global war' against terrorism. As the examples in this thesis suggest, the support of a nation-state is not a requirement for severity when it comes to cyber-attacks, or in fact any kind of attack, since in many cases the sponsorship of the state cannot be proven. As the example of the criminal group RBN later in section 3.1.2 will prove, state sponsorship cannot be a precondition for a serious attack.

2. Consequence: Did the attack cause harm?

This is another doubtful test since even a hacker can cause harm by infecting a computer with malware (malicious software) or defacing a website. On several scenarios serious physical damage could ensue (e.g., interference with air traffic safety). While a less damaging attack may be less likely to get publicized (Bosch,2004, p. 188), the 'seriousness' with which a victim state regards it is not necessarily tied to the level of direct harm, being linked with feelings about the possible culprit, sense of vulnerability, fear of future attacks etc. In the Estonian case most important websites were only offline for a few hours or days at most.

[7] Report available at URL: http://resources.mcafee.com/content/NACriminologyReport2009NF

Yet this is considered one of the most serious cyber-attacks performed. The psychological effect can perhaps be compared to a home invasion. If a burglar enters your home, but steals nothing and damages nothing, is the home invasion not serious?

3. Motivation: Was the attack politically motivated?

Although the 'political' term is quite wide and can cover many scenarios, this still seems to be quite a narrow definition. As has been pointed out earlier there are cyber-criminals, such as hackers, who carry out attacks without any other apparent reason than for destruction. To call such an attack political could perhaps be a stretch, but that still does not mean that the attack or incident would not be experienced as having a warlike effect. There is also the mercenary factor, which may influence the people leasing the tools and executing the attack even if not applying to the prime mover.

4. Sophistication: Did the attack require customized methods and/or complex planning (McAfee Inc., 2009, p. 8)?

Most cyber-attacks can be performed with a standardized toolkit that can be found with a simple Google search. To assume that no serious harm can be done with such simple means would seem to be presumptuous. There is also the question of how 'complex' planning is required to be in order to be called sophisticated. Just going on-line and finding the tools, setting the target and executing the attack is a significant sequence of actions that would not happen by accident. Most if not all of the instructions and tutorials about how and when to attack can probably be found on forums and other websites, so by that logic the skill of any cyber-attack could not really be considered sophisticated.

Using these four attributes, the specialists at McAfee decline to describe the cyber-attacks described in this chapter, that is on Estonia, Georgia or the 4th of July attacks on the US and South-Korea, as actual cyber-warfare. That is mainly because of the lack of proof that the attacks were committed or sponsored by nation-states. But as has been stated before and will be explained further in this chapter, one of the main benefits of using cyber-attacks is the fact that the real promoters can be masked. In the case of Russia and the Russia Business Network (RBN), evidence suggests that Russia and the cyber-criminal organization are bound together at the least by politics and money. The fact that the connection cannot really be proven has significant but interesting results, as the RBN is

thought to be responsible for some of the greatest cyber-attacks in recent history, perhaps with greed as the only motive.

3.1.2 Ideological and political extremism

The opportunities given by globalization and the expansion of the Internet have not been ignored by terrorist groups. The actual crimes committed by such groups may not differ greatly from 'traditional hactivism', such as infiltration of computers and credit card fraud. The difference lies mainly in the motives behind the crimes, as the infiltrated computers are often used to distribute terrorist material (video files, instructions, etc) and the stolen credit card information is used to fund terrorist activity, such as the upkeep of terrorist-message websites (Cornish, Hughes, & Livingstone, 2009, p. 5).

The Internet originated in the Cold War and was supposed to work in the event of a nuclear attack (Cornish, Hughes, & Livingstone, 2009, p. 5). Its resilience, speed, and low cost of use are appealing to terrorist groups, just as any other group. The fact that the Internet is mostly 'ungoverned' (little regulated and not policed by any traditional official authority) certainly appeals as well. The Internet helps also to coordinate terrorist organizations that are looser and more opaque in their structure (Cornish, Hughes, & Livingstone, 2009, p. 5). Coordination, training and even recruitment are made possible over the Internet with the help of forums, blogs, media groups, etc. Matters can be discussed in real-time between members to give the impression of democracy. The Internet also makes the distribution of propaganda much easier, and keeps it available over time for anyone interested - at no extra cost (Cornish, Hughes, & Livingstone, 2009, p. 6).

The Internet has also facilitated communications between different terrorist or extremist groups (Stern, J, 2003). Information sharing between groups that don't necessarily have the same enemy is not outside the realm of possibility. For instance, Louis Beam, a self-proclaimed computer terrorist for an American neo-Nazi group, wrote an essay about 'leaderless resistance' and this essay has also been very popular with radical Muslims (Stern, J, 2003). Beam writes that a hierarchical organization can be very dangerous for a terrorist group because technology can provide information about the structure of the organization, thus

exposing it. In a leaderless organization, each cell works independently and never reports to any central headquarters or single leader. This essay has been available on radical Muslim sites, along with training courses about how to make explosives and how to inspire the creation of more cells. Using the Internet has also provided better 'leaderless resisters', as they are often better educated than those that are recruited by the traditional methods such as radio programs (Stern, J, 2003). The Internet has also made it easier to recruit in different regions, where there is less suspicion and surveillance than for instance in the Middle East. The vast array of information available through the Internet makes it possible for anyone to learn about the message that groups like Al Qaida are preaching, and many people would probably say that that is a bad thing. Many extremist groups have supported the September 11th attacks or Al Qaida as a shot against globalization, as globalization is thought to exterminate national cultures. (It is of course ironic that this acclaimed shot against globalization is celebrated through the Internet, one of the greatest tools of globalization.) Leaderless resisters from white-supremacist groups are not thought to be able to carry out massive attacks alone, but with cooperation and planning by Al Qaida they are certainly thought to be more dangerous, and with the help of the Internet, that planning is made more possible (Stern, J, 2003).

The Internet has in a way become a virtual training ground where members of terrorist groups can find manuals and simulators to train for any task that they might face. The Internet has also been made part of messaging campaigns by Al-Qaida and other extremist groups (Cornish, Hughes, & Livingstone, 2009, p. 6). It allows individuals in small and/or remote cells to operate without direct command, and possibly with quite different motives. The danger of the Internet in this respect is that it places weapons in the hands of any individual who searches for them. In recent years there has been an increase in websites on Islamist extremism in western languages, seeking to attract a western audience. The Internet also makes it possible for small separatist groups to claim responsibility for attacks and to try to bolster their reputation (Europol – Terrorism Situation and Trend Report 2009, p. 40[8]).

[8] Report available at URL: http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/TESAT2009.pdf

There are several known examples of how extremist Muslims have used the Internet. There is for instance the 'Muslims Hackers' Club', which offers radio frequencies used by US Secret Service Agents. There can also be found tutorials and manuals on hacking. Irhabi007 is one of the most famous Muslim cyber-criminals. He used forums and websites to provide manuals and videos in support of the extremist Muslim cause, and has been said to have brought the Jihadist into the twenty-first century (Center for Strategic and International Studies, 2008, p. 4). In 2007 Irhabi007, real name Younes Tsouli, age 23, was sentenced to 16 years in an English penitentiary.

In reference to the question of whether a successful 'large-scale' cyber-attack could be considered an act of terrorism it can be helpful to look at the definition for terrorism set forth by the United Nations.

> Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them; (United Nations General Assembly, 1995)

It is clear that a well organized cyber-attack, such as the one against Georgia, has the potential to inflict the terror the resolution speaks of. The UN definition states that the acts should be done for political purposes, but the difficulty of proving this in the special case of cyber-attacks has already been discussed and the victims of an attack resulting for instance in destruction of critical infrastructure might feel even more terrorized if unsure which enemy was attacking them and why. Although the threshold for what can cause terror within a community can often be quite low, it must be better to keep that threshold low rather than to have it high, and allow people to be in a constant state of fear.

Although terrorist groups and other extremist have taken to the Internet on a large scale, it may be questioned whether that move was made by will or under duress. Have terrorists turned to the Internet because it works for them best, or because all other places have been closed? If the latter were true, cyber-methods could be seen as a 'last refuge' for terrorists with the hope that tackling them on that ground could eradicate the threat forever. But there is also the other

possibility that terrorist groups have flocked to the Internet because it is a very good forum for coordination and planning, which complements or even increases their strengths in other domains. Time will hopefully tell which view is correct.

3.1.3 Serious and organized crime

As the Internet has become the scene for such a large part of normal people's transactions it is hardly surprising that criminal interest has followed. The possibilities the Internet offers, for instance to transmit funds without drawing the attention that application to a bank would cause, certainly is appealing to organized crime groups (Cornish, Hughes, & Livingstone, 2009, p. 7). The connection between 'cyber-criminals' and 'cyber-law-enforcers' is a peculiar one, where the actions of one actor bring the reactions of the other actor in a seemingly endless circle. The objects that are most highly defended by law-enforcement agencies are often most coveted by criminals, and so a cyclical trend emerges, as law-enforcers try to defend, and the criminals try to steal (Cornish, Hughes, & Livingstone, 2009 pp. 7-8).

Spam is the most basic form of cyber-crime, and in many respects is also the most serious. Spam is reported to be around 94% of all email traffic and is used to deliver viruses and Trojans (Cornish, Hughes, & Livingstone, 2009, p. 8). These viruses 'phish' information from the infected computers, making it possible for the creators/senders of the virus to collect and sell the data on the cyber-black-market. There is a large market for stolen banking information, credit card information, personal identification numbers, etc (Cornish, Hughes, & Livingstone, 2009 p. 8). These same infected computers can also be sold in botnets (robot networks), where the original criminal can use them for his own purposes or lease them to others. From July to December 2007, Symantec detected 62.000 active bot-infected computers each day (Cornish, Hughes, & Livingstone, 2009, p. 8). All of these 62.000 computers could be directed to visit any site or server that can be accessed from the Internet, for example the website of the Foreign Ministry of Iceland, causing it to overload and forcing it offline. This is what is called DDOS, or Distributed Denial of Service. In the cases when the attack is based on only one computer it is referred to as a Denial of Service attack, which is, not being distributed. Obviously these botnets can be very valuable to the owner, as they can also be used to distribute more spam, infecting

more computers, or they can be used to gather more information that can be gathered and sold (Cornish, Hughes, & Livingstone, 2009, p. 8). The damage caused by such methods can be counted in the millions of dollars.

Even though the 'serious' and 'organized crimes' label carries some connotations, the matter is somewhat muddled in cyber-space. Crimes need not be very organized before they are serious, or organized crimes need not have any particular level of sophistication (Cornish, Hughes, & Livingstone, 2009, p. 9). Lower-level criminals can be part of a larger crime that becomes serious through its scale. It remains to be seen whether cyber-crimes will remain basically a repetition of older crimes in a new costume, or whether they will evolve into something new. Given the continued evolvement of cyber-matters, nothing can really be taken as a surprise.

Older serious organized crime groups such as the Asian triads, the Yakuza or the Eastern European organizations have moved onto the Internet in a way predictably reflecting their respective criminal enterprises (Cornish, Hughes, & Livingstone, 2009, p. 9). Although the Internet may help them to jump from jurisdiction to jurisdiction, some of these older groups retain their older networks and methods and have not gone completely on-line. This provides opportunities for law-enforcement that a complete cyber-presence by these groups would not allow.

Darkmarket could be taken as an example of how organized crime can work, but also how international cooperation in law-enforcement can prevail against cyber-criminals. Darkmarket was a website founded and run by a Sri Lankan immigrant, working from a coffee shop in Wembley, United Kingdom. The site was only accessible by invitation after scrutiny, but once in, the members had access to roughly 2000 other members, each having something to offer: stolen credit cards, tutorials in account takeovers, money laundering, and even offers to buy fake ATMs and pin machines (Davies, 2010). The system was based on a pyramid scheme, meaning that the highest ranking members of Darkmarket received a part of whatever lower ranked members earned from using the site. Strict rules were upheld on the site to try to keep it from the public eye, such as restrictions in commerce in firearms, drugs and counterfeit money. There were

also strict regulations against ripping off other members of the site. On the Darkmarket site a price list could be found, where for example renting a botnet for one day would cost 50 dollars. That price could probably change somewhat with the added size of the zombie army, but this is certainly a good reference point. Information about credit accounts that could be taken over would range from 150 to 300 dollars, depending on how much the balance of the accounts would be (Davies, 2010). Although this was one of the top ten sites in the world when it comes to cyber-crimes, there are still more than a hundred more that are known, and then probably around the same amount of unknown sites.

Crimes that have such a spontaneous nature as cyber-crimes are certainly hard to fight. Groups can be formed and disbanded for ad hoc missions, leaving near to no traces. This requires that law-enforcement work in a similar fashion, preferably working without a cumbersome infrastructure and being able to respond as the crimes evolve. One clear example of the spontaneity of cyber-crimes can be found in RBN, which both acted quickly when it came to attacks and when it was finally cornered, was also quick to vanish almost without a trace.

3.1.3.1 RBN

The Russian Business Network, or RBN, could certainly be said to look like something out of a suspense thriller or a huge Hollywood movie. This is an excellent example of the possibilities of organized cyber-crimes with an added ‘state factor’. While there are perhaps several online criminal organizations, few have reached the level of effectiveness the RBN has achieved, as will be explained in this section. The RBN has also been named as a possible culprit in the cyber-attacks against Estonia and Georgia, which will be discussed in section 3.2.

The group first drew attention in 2007, though presumably having been around for longer, and is fronted by an individual called ‘Flyman’. Much that has been said about this group of cyber-criminals is naturally hard to prove, but certain charges have been stated too often to be ignored. The RBN have been called the ‘baddest of the bad’ when it comes to Internet activity (Miller, 2007). The group has been involved in cyber-fraud such as phishing sites and Trojans, malicious botnets and child pornography as its usual modus operandi, along with

the occasional protection racket and harbouring cyber-mercenaries (Keizer, 2008). According to one report, a group that solicited RBN services for phishing made 150 million dollars in one year by tricking people into giving them their banking information (Blakely, *et al*, 2007). There are rumours that the RBN has connections with the Kremlin, which might explain why its members have never been apprehended (Miller, 2007). There are also reports that the group has simply bought the services of the local police, judges and government officials in its hometown of St. Petersburg – which in the allegedly corrupt Russian environment would also explain the lack of arrests (Leyden, 2009a). Even if the group is basically independent of the state, it may still be exploited by the authorities as a deniable agent or at least as a plausible scapegoat. Although the RBN are said to have been making millions of dollars a year from cyber-crimes, they are also said to frown upon stealing from great numbers from individuals, preferring to attack banks and other larger corporations where the customer is still compensated in the case of cyber-fraud (Miller, 2007).

In most cases the methods of the RBN are similar to methods of traditional organized crime groups, enhanced by the cyber-aspect. The protection racket of the RBN is said to be so organized that while one hand performs a DDoS attack against a site, the other hand offers protection against such attacks for a price of 2000 dollars each month (Keizer, 2008). This is possible with the anonymity of the Internet and the fact that the RBN have a vast array of websites that are used to host various criminal activities, such as online pornography, pharmaceutical sales and 'HYIP' – High Yield Investment Programs, traditional online scams that often involve promises of great returns in a short time (Keizer, 2008). It is also interesting to note that although this is certainly an active and large criminal organization, it still has a somewhat 'small-time' philosophy. Reports state that some attacks performed by the RBN are performed because of the vanity of 'Flyman', the leader of the RBN. For instance, when RBN attempted an attack against a Pakistani bank but were rejected, 'Flyman' was reportedly determined to try harder to prove his ability (Malik, 2010).

The connections the RBN has with the Russian elite have made it near impossible for international law enforcement to land a successful blow to the organization. All that was possible was to disrupt the works of the RBN, for

instance with high-profile news articles about the organization, and in 2007, the RBN executed a disaster recovery plan, effectively moving from Russia. It has also been speculated that the group had attempted more than it could handle, angering many foreign governments instead of only corporations (Espiner, 2007). One of the last hacks the group performed before they moved from St. Petersburg was against a site belonging to the Turkish government, redirecting traffic to a RBN site that distributed viruses, and this action is believed to have led to the RBN's political protection being withdrawn (Espiner, 2007). After some initial difficulties the group managed to go into hiding, either disbanding or possibly hiding on Chinese servers, (Leyden, 2009a) as identical activity started almost at once from IP addresses registered in China and Taiwan (Carr, 2007). Here the nature and difficulty of cyber-crimes is clearly manifested, as the criminal does not really need a physical location. The only thing that is needed is a computer and an Internet connection. And without a prison sentence, cyber-criminals really have no real incentive to leave the field.

The founders and main members of the RBN are said to be young computer science graduates, who in other circumstances might be setting up the Russian Google or an equivalent (Warren, 2007). When the group was first set up its focus was not entirely illegal, but as time went on the members saw that is was much more lucrative to move into the illegal sphere. More money meant that the group could recruit the top graduates from the universities, successfully offering them salaries greatly above anything else available (Warren, 2007). By 2007, not one legal affiliate could be found in the group yet the members kept up a certain law-abiding image. For instance the group rented out 'bullet-proof' servers for anyone who was interested, but in the case of an accusation took the server down, only to be returned a short time later[9]. That allowed the RBN to claim that they were following the law, while still hosting the servers (Warren, 2007). As already noted, the group also had principles about who could be attacked and among other things frowned on attacks within Russia, which may have helped to keep the local police on their side. Their main victims were the banks of westerners, so that the RBN could even be seen by some as 'freedom-fighters' (Warren, 2007). Here

[9] Other examples of 'bullet-proof hosting' include offering renters the chance to clean out their servers before they are closed or offered to law-enforcement.

certain similarities can be seen with Darkmarket mentioned earlier in this section, where adamant rules were against any type of crimes against fellow-criminals. This trend can be seen in other aspects of cyber-crimes[10].

Many ordinary Russians would also approve if the RBN were indeed involved in the attacks against Estonia and Georgia as is claimed later in this chapter. The reluctance of the Russian police to aid international efforts against such criminals has often caused friction and resentment, although another more creditable explanation could be that the police had their own investigations under way and did not want foreign action to cut across them (Krebs, 2007). As will be explained in section 3.2, Russian guilt for the cyber-attacks against Estonia and Georgia can hardly be proven, and therefore it is also difficult to prove if the RBN acted on behalf of the Russian state.

After remaining in hiding for almost two years, the RBN are believed to have returned. Citigroup, the world's largest financial service company, is believed to have been hacked and tens of millions of dollars stolen (Johnson, 2009). Specialists are sure that this marks a return for the criminal group, although – as often happens, the company has declined to confirm it. There are commercial dangers in a firm's admitting that its systems have been infiltrated and are not secure (Bartz and Finkle, 2009), and in Citigroup's case reporting a crime could hurt the company, shareholders, and in the end probably the customers in terms of interest rates and such. Yet reporting the crime could also harm the perpetrators, whereas not reporting the crime lets the criminals go free.

It is actually possible to defend against groups such as the RBN. When an ISP (Internet Service Provider) knows the IP addresses[11] of a group such as the RBN, access to these addresses can then be closed. Examples have shown that when access has been limited, less time and money has been spent cleaning computers from viruses caused by RBN computers (Krebs, 2007). The difficulty that can emerge in this case is that the ISP takes on itself the right to close access to certain addresses for its customers, in the name of protecting their safety. The tension between the people's rights and their freedom is an old but recurring one,

[10] It is known that some malware will not be installed if another malware is already present on the relevant computer. The computer is considered 'owned' and thus will not be touched.
[11] Internet Protocol – An internet address of sorts.

and also one that can hardly be resolved without a verdict or agreement from above. If an international agreement was available allowing but regulating such preventive action by service providers, the matter would look quite different (Krebs, 2007). Both NATO networks as well as private anti-virus networks frequently share lists of malicious IP addresses.

3.1.4 Lower-level/individual crime

This can be considered the lowest level of the cyber-crime spectrum. The public preconception, as Richard Clarke maintained, is of a teenager with too much time on his hands. The truth is more often that the hacker can be highly educated and skilled in programming (Cornish, Hughes, & Livingstone, 2009, p. 11). In the hierarchy of computer crimes, the inexperienced teenager is usually called a 'script kiddie' because he is likely to borrow scripts from other hackers and may not understand how the tools he is using work – let alone what the real consequences may be (McAfee Inc., 2005, p. 10). Yet an individual who does not understand the effects of his own actions can often be extremely dangerous. The reasons behind a hack can be diverse, from possible financial gains to group celebrity status to the simple taste for destruction. Then there could also be the disgruntled employee on a quest for revenge or a disappointed customer (Cornish, Hughes, & Livingstone, 2009, p. 11).

These hackers, although low-level, can be integrated into larger groups and campaigns and in that case are definitely dangerous. The individual hacker is the building block of every other cyber-crime, and the simplest hacks are often a great source of funds for the larger organizations and groups. Insider threats can be especially dangerous, and despite the preoccupation with intrusion by malware, over 80% of unauthorized access to files happens because of insiders. Most often employees committing acts of this kind have shown signs of bad behaviour before. Financial losses, negative publicity and loss of image and goodwill can be caused by this behaviour, and in times of recession this is even more damaging (Council of Europe, 2008, p. 45).The insider can also provide access to corporations by accident. If the corporation network is not secure, documents can be accessible without much effort. There is also the added fact that many companies offer laptops for their employees, and while laptops are quite often stolen the employees could be unwilling to admit to this theft. These laptops, as well as

other data storage devices, contain valuable information that could be used for extortion purposes. Recently the British government faced serious embarrassment because of lost laptops and USB memory sticks that had carried sensitive personal data among other things (Council of Europe, 2008, p. 47).

In times of recession the habits of people are bound to change in some way, and this is also true for cyber-matters. When corporations are forced to decrease spending there is a tendency to cut corners in cyber-security. Security technicians would strongly advise against this and on the contrary, argue for more efficient security and better control of the environment to prevent security breaches. Again, some people losing their jobs through a recession may turn to crime. Organized crime groups also experience recessions and people have less money to spend on drugs and prostitution. These crime groups are then forced to try to find other ways to earn money (Espiner, 2008).

The vulnerability of cyber-records to hacking and threat is more serious in some areas than others: for instance in the case of medical records, which have increasingly been digitized to ease handling (Brewin, 2009). It has been demonstrated on several occasions, for instance with the outbreak of anthrax following the 9/11 attacks, that a relatively small incident can cause panic on a large scale, even more so when several small incidents coincide. Panic can then spread through communities and even nations. Unlawful access to computerized medical files can allow a hacker to alter prescriptions, change allergy information, change diagnosis and even access medical equipment (Brewin, 2009). Although these can be considered small crimes *per se*, the effects could be extensive. In particular, the impact on patients' confidence in doctors can be imagined if unusual medical incidents proliferated across the country. Failure within the infrastructure can spread quickly.

Another aspect of the actions of individuals on the Internet is cyber-bullying. The Internet provides an anonymity that can make cyber-bullying particularly difficult to fight. Online forum- and network site posts and anonymous text messages are only a few of the ways that cyber-bullying can present itself. Technological advances make communications work faster, and the fact that a person can record a video on their cell phone and send it on the Internet

in a matter of seconds can make cyber-bullying very easy. The possibilities involved are not all negative: for instance, public officials could be said to be under more scrutiny since the methods to record and publish their action have become easier. Yet the way has been opened up for possible invasion of privacy on a vast scale. The only way to prevent cyber-bullying, short of some kind of restricted access to cyber-media, is education on the consequences. This of course is also true of physical bullying and underlines that online offences are often different from real-life ones only in the medium used. Education is actually a valuable part of the solutions to many cyber-issues.

3.1.4.1 Fraud on the Internet

Phishing and Pharming are common cyber-crimes that yield high profits for criminal organizations, and have become more advanced in recent years. Phishing revolves around stealing credit card numbers and other information that can be used to extract money. It is also clear that if a criminal enterprise has banking information all around the world, that information can be used to launder money perhaps coming from ill-gotten sources. Among the methods for phishing are mass e-mails that are sent to customers of banks where the customers are asked to verify that certain numbers are correct, or are asked to send other account numbers that can be used to extract money. Although most people have figured out that these are actually scams, there are still some who do send the requested information. While the cost of sending these mass emails is still virtually none, any account information can be counted as a benefit for the criminals. Major events in the world are often exploited to phish information, thus letters asking for donations in aid of the people of Haiti, allegedly going through the Red Cross, became common in early 2010. Celebrity news also provides an opportunity, with the death of Michael Jackson resulting in a huge increase in spam. Phishing methods try to appeal to basic and common human attributes; namely greed and curiosity. It need not come as a surprise that these methods are still working. Another method that is quite popular is connected with special holidays. When February 14th rolls around, it can almost be counted on that there is great number of infected websites offering Valentine's Day gifts of some sorts. Advances in phishing methods often make it impossible to see whether the information request is actually from the claimed sender (HTCC Threat Assessment 2007, p. 27).

Instructions about how to start phishing are freely available online, and can be accessed with a simple Google search.

Examples of pharming are for instance if a virus changes the bookmarks of the infected computer, redirecting the user on to a dupe site. That site would then look exactly like the real site but when the user puts in the required information, the virus logs the information, and the user is unable to log into his site. These fake sites often have more hidden traps that can infect the computers even more, making them even harder to clean. The problem is aggravated because, as noted, banks are perhaps reluctant to admit that their sites have been used to try to scam people, opting rather to manage the matter themselves (HTCC Threat Assessment 2007, p. 29). Although of course it is good that the matter is dealt with in some way, the general public is left without the necessary warning and knowledge of cyber-dangers. Similarly, individuals are often not willing to admit that they have been victim of computer fraud, blaming themselves for being tricked. Internet Service Providers could also be unwilling to admit that their service has been attacked, fearing that clients would transfer their business to another ISP. Better education could always make a difference, as individuals would be more educated on the dangers of the Internet, and would know where to report if they have become victims of cyber-crimes. ISPs and other institutions would also be more willing to report the threats, as an open dialogue would reveal that cyber-threats can affect anyone.

To a certain degree the so called ‘Nigerian scams’ could be called online fraud. The modus operandi in a Nigerian scam is that a letter is sent to a person, where that person is asked to aid in moving funds, often from a poor African nation. The sender is often said to be an heir to millions of dollars, but being unable to get the money himself needs the help of an outsider. All the sender of letter needs is a small fee for certain licenses and bribes, and then when the millions are in the heir’s hands, the helper would get a sizable percentage for their help. Of course when the sender receives the money from the helper, that money is lost forever. Although the awareness of these types of frauds is increasing, there are still some people who are deceived by these letters. Translation sites, such as translate.google.com, are making it harder to spot such letters which were once normally written in bad English but can now be sent in any language, even an

obscure one like Icelandic. The difference between this type of fraud and for instance phishing is that the Nigerian scam does not depend on the use of a computer but is merely made faster and easier by it. The letter could certainly be sent by old fashioned mail, and the money transferred could be sent by many different means. This brings up a point mentioned in a previous chapter, that some of the so-called cyber-crimes are really just new renderings of older crimes. The cyber-aspect just makes the scam easier to manage and cheaper to produce.

The amount of sites online that are used for illegal activity can be disputed, but there are signs that the vast majority of registered sites are actually used for criminal activity. 77% of sites have been thought to have been registered with false or incomplete information. Although this in itself is not a sign of criminal activity, roughly 30% of the sites are registered with information that is clearly fabricated or suspicious (McCarthy, 2010). It has been estimated that online fraud is costing the British Internet users around 3.5 billion pounds every year, scamming approximately 3 million people every year (West, 2010). This has to be considered peculiar as most Internet users should have at least heard of the dangers of the Internet, and other threats that have received such an extensive publicity as cyber-threats are hardly claiming as many victims.

3.2 Methods of Cyber-attack and nations as targets

The main technical categories of cyber-attacks and –crimes identified by security experts and computer technicians will first be recapitulated here, pulling together the examples mentioned in passing in the previous section. Many of the methods might be employed at once by the same individual or group, such as the Russian Business Network already discussed. The remainder of the section offers some real-life examples of attacks made on states using some or all of these methods.

Distributed Denial of Service (DDoS) is a rather simple procedure that can cause substantial damage, as already mentioned. A DDoS attack is for the most part based on the most simple of cyber-threats, spam e-mail. Other ways include simple communications between computers that can be overwhelming in vast quantities. Spam is the tool most often used to infect a computer with viruses and malware that make it part of a botnet and usable in a DDoS attack. When attacked and overloaded by a botnet, the targeted computer cannot distinguish the latter

from real traffic and can only respond by disconnecting or shutting down fully, thus blocking legitimate use as well (European Commission, 2009, p. 74).[12] While the actual attacking computers might be detectable and traceable, the individual or group operating the botnet can effectively hide from being found. Any computer that can access the Internet is open to such intrusion but may be protected by firewalls and other security systems available for procurement.

The average botnet can be used for industrial espionage, information phishing and extortions. The two most infected countries in the world are the US and the United Kingdom. In 2005 the United Kingdom jumped to first place on the list because of an increase in bandwidth that was available (HTCC: Threat Assessment 2007, p. 20). More bandwidth makes it possible for more computers to be online at the same time, thus making more computers available for the botnets to infect. This raises an interesting connection with the discussion on risk in the previous chapter. In this case, a decision to provide added bandwidth for the country also increased the risk of computer crimes in parallel. This can often be the case when it comes to technological advances, anywhere in the world including Iceland. Finally, it should be mentioned that computers are becoming even more common with every passing year. Many countries in the developing world are becoming rapidly computerized and with each country that does so, the more dangerous the Internet becomes. Security measures are not likely to be as rigorous in the developing as in the developed world, and the day when the international community demands anti-virus software for all could be a long time away.

Botnets, like most aspects of cyber-threats, are very hard to fight because of their international nature. Transnational cooperation is increasing when it comes to fighting botnets, for instance because in order to close down a botnet, the Command and Control server must be found[13] (HTCC Threat Assessment 2007, p. 25). Important steps have been taken all over the world by Internet

[12] Report available at URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

[13] The Command and Control server is the server that controls the actions of the infected computers. While the infected computers can be found and taken offline, no victory is really won until the command server has been disrupted.

Service Providers (ISPs) to limit vulnerability to spam, which in turn reduces the chance that a computer could become a drone in a botnet. The cost for an ISP of protecting its own system and the computers of its clients could be extensive. In times of recession companies try to keep cost as low as possible, and as has been stated before, security is too often one of the first to be sacrificed.

Although criminal organizations are keeping up with technological trends when it comes to cyber-threats, the security experts are also advancing. While the criminals are moving onto fields such as VOIP (Voice over IP service, Internet phone calls) or mobile phones to attempt to scam people of their money, the banks are starting to use simple tools that make it more difficult for criminals to fake their website successfully. There have been examples of cyber-criminals successfully infiltrating online-banking of individuals in Iceland. That problem has mostly been avoided with the distribution of a small ID unit that was given to all bank account holders in Iceland, increasing the security immensely. This has dramatically minimized bank fraud in Iceland (Foreign Ministry of Iceland, 2009). However, as criminals seek ways to overcome a new defence, the cycle can go on for some time. The same can be said about ISPs, as with every security door that the ISPs successfully close, the cyber-criminals have found others to open. This then means more expense for the ISPs.

The last type of offence to be mentioned here is the trafficking of child pornography. This is distinct from what is normally defined as cyber-crime but is often linked with it, as some sites offer storage of child pornography and the tools for hacking at the same place (HTCC Threat Assessment 2007, p. 40). Things like anonymity and secrecy are beneficial for both the pornography distributor and the cyber-criminal. The digitalization of child pornography has made the matter even more difficult, as a single picture can be copied thousands of times, victimizing the child just as often. Most of the latest technological advances can be used by criminals to try to ‘groom’ and lure children, such as VOIP, MSN and Skype. Peer-2-Peer networks are also making it more difficult for law enforcers to fulfil their obligations completely, and they can often only reach the criminals through further cooperation with ISPs. The trafficking of child pornography may also be a stepping stone to other related crimes, for instance the trafficking of human beings and extortion. Conversely other cyber-crimes, such as phishing, create revenues

for these criminals' activities to continue (HTCC Threat Assessment 2007, p. 42). Regular credit cards are still being used to purchase access to child pornography, and that makes it possible for banking agencies to work together in an effort to apprehend these criminals, both the sellers and the buyers. These are the cyber-threats that concern the regular individual.

A larger aspect of cyber-threats revolves around international transactions, for instance among states. There are examples of cyber-attacks against states that are not considered serious, although the reasons for that categorization can be disputed. On the 4th of July 2009, several US websites and government institutions, for example the White House, Department of Homeland Security, The US Secret Service, The NSA, and the Departments of State, Defence, and the Treasury were all attacked at once, but the results went largely unnoticed because people were celebrating the National holiday. If occurring on a normal working day, the 4th of July cyber-attacks would perhaps be considered the most serious cyber-attack to-date (McAfee Inc., 2009, pp. 4-5). The following day several sites in South Korea were attacked by a net of 50,000 computers. Although the attacks could not be traced, the computer attack was blamed on North Korea. Most of the attacked websites were back online in a few hours, and the results were hardly more than a nuisance for the US and South Korea (McAfee Inc., 2009, p. 5). There has been speculation on the motives, since any attacker must have known the date of the US national day. One theory is that the attacks were supposed to be more serious and would then profit from the fact that the level of defence could be lower on that particular day, so the attacks could go on longer before counter-measures would be taken. Another theory is that the attacks were only intended to test the security network of the US, seeing if there were any weak points that could be exploited in later attacks that would then be executed with even more force. What can safely be assumed in any case is that the cyber-defence of the affected websites and institutions must have been increased in the aftermath of these attacks.

Several other cyber-attacks on nations have taken place in the last years, many of which probably go unnoticed or unreported. A few however have attracted international attention and helped to trigger debate on cyber-threats as an

international concern, and the best known examples will be examined in this section. They do of course vary in severity and coordination.

3.2.1 Malaysia

The cyber-attacks on Malaysia offer a good point of reference as to the peculiarities of this type of threat. Here is a rather small group of hackers managing to deface a large group of computers for a small country, and making a significant mark on the scene (Kian, 2009).

On August 31st 2009, the national day of Malaysia, several governmental sites were attacked by what seemed to be a well coordinated effort. The effort was actually coordinated by Indonesian hackers who claimed that Malaysia had treated their citizens and migrant workers poorly in the past, and wanted to make the Malaysian people and state pay for their alleged crimes. The effects of the attacks were not substantial, as most official sites were soon returning to normal. Only a few private sites still displayed a message from the Indonesian hacker group. Later the foreign minister of Indonesia claimed that the hacker group was composed of young people who were acting out of emotion rather than rationality, and called for everyone to remain calm. As far as the Malaysian authorities are concerned the matter was not pursued further.

This attack, although relatively mild in severity, reflected a particular inter-state dispute but one where citizens seized the initiative – a much more uncommon phenomenon in traditional warfare. In the case of Malaysia, even if a few troubled youths were the perpetrators, they may be looked at as the foot-soldiers of all cyber-threats and could have caused much more damage in larger numbers (as happened in other cases cited below). Moreover, if Malaysia had assumed from the beginning that the Indonesian state was behind the attacks, this could have led to a real inter-state dispute. The two countries being neighbours, the matter could have escalated quickly (Karana & Andriyanto, 2009).

3.2.2 Kyrgyzstan

Kyrgyzstan can hardly be called an important actor in the international system. The country is wedged between China and Kazakhstan, and is not rich in any natural resources. The country is not at war with anybody and it is not very Internet capable, as Estonia is for instance. The cyber-attacks on Kyrgyzstan have

been described as the attacks that no one knows about, compared with the more famous and somewhat parallel cases of Estonia and Georgia. It can be assumed that the cyber-attacks against Kyrgyzstan were indeed perpetrated by Russia in an effort to frighten the Kyrgyz government without exposing Moscow's hand directly. Another theory is that the attacks were not intended for the government of Kyrgyzstan as such, but were rather intended to frighten the oppositional parties who were rumoured to be working at establishing an oppositional coalition, the United Peoples Movement, expected to be more pro-West than the presiding government (Mamatov, 2009). Yet another theory could be that the attacks were staged by the Kyrgyzstan government themselves to strengthen Russia's enemy image and gain popular support for siding with the US against Russia (Bradbury, 2009). No option can be ruled out because of the special difficulties of identifying a cyber-attacker, something that can foster insecurity and danger in itself.

Analysts have traced the attacks to the Russian Business Network that was discussed earlier in this chapter. The Russian Business Network is thought to have been working on behalf of the Russian government in this and other cases, but using a third party like the RBN gives the Russians a plausible deniability (Bradbury, 2009). The reason thought most likely in that light is traced to Russia–US relations, as the US military has a military base in Kyrgyzstan that Russia does not like to have on its doorstep. Russia tried to offer debt write-offs and investment opportunities to persuade the Kyrgyz authorities to close it, but in the end an offer of higher payments from the US was accepted and the base remains (Schwirtz & Levy, 2009).

As Kyrgyzstan has only four ISPs (Internet Service Providers), attackers really only have to focus on these four targets to cripple the Internet access in the entire country to an extensive degree. In this case the attackers actually infiltrated two of the four ISPs, and the only thing that is said to have helped Kyrgyzstan is that the online services in Kyrgyzstan were bad to begin with (Jenik, 2009). It should be pointed out and will be addressed in later chapters that the ISPs in Iceland for the most part are only 3, with a few smaller ones having a very small market share and mostly relying on connections with the larger ones. This could make Iceland even more vulnerable than Kyrgyzstan.

3.2.3 Estonia

The trigger for the cyber-attacks of 2007 against Estonia can hardly be considered modern or technological in any way. A bronze statue in the old town centre of Tallinn, the capital of Estonia, was finally to be moved from its high profile place to a lesser location. The bronze statue had a lot of history. Named the 'unknown soldier' by the Russians when they erected it in 1947 to memorise the 'liberation' of Estonia, it was of course never popular with the Estonians. They named it the 'unknown rapist', and for the years of Soviet occupation and after the end of the Cold War, the statue was the meeting place for Russian centric minds in Estonia, along with the roughly 400.000 Russian speaking inhabitants of Estonia (Ruus, 2008). And in early 2007, with Russia in debates with the EU over gas supplies and Estonia looking more and more to the West, the bronze statue was more and more personified as the legacy of the old regime. It was finally decided to move the 'unknown soldier' to a military cemetery on the morning of April 27th, 2007.

The reactions were very quick to appear. In Tallinn there were riots and looting, with the police using tear gas and water hoses to gain control over the people. One person was killed. In Russia the Estonian embassy was blockaded by thugs for some days (Ruus, 2008). When the physical rioting and attacks were subsiding it became clear that a cyber-attack was under way, and it was escalating. For some days before the moving of the bronze soldier many Russian sites were aflame with cries for vengeance upon the Estonians for their disrespect (Ruus, 2008). Websites offered detailed information about what sites should be attacked and even offered the tools necessary to commit the attacks, which were mostly DDoS attacks. The main targets of the attacks were the Estonian presidency and its parliament, most of the country's ministries, Estonian political parties, half of the news organizations, banks and communication companies (Traynor, 2007).

These are obviously important sites, and by any nation's standards this would be a serious attack. But the impact on Estonia was even more serious because this relatively small nation of 1.4 million had been a pioneer in 'e-governance' and was exceptionally 'wired up'. Around ninety-eight percent of banking transactions are performed online, the Estonians can vote in both local and national elections online and more than ninety percent of the taxes are filed electronically. The Estonian government was paperless, meaning that all official

documents were produced and published electronically (Reinart, 2009). As was stated in the Risk section of Chapter two, the more a nation relies on something, the more vulnerable they become in that respect. This was certainly true in the case of Estonia. But despite the vulnerabilities, the training of the Estonians also made them quicker than others to respond to the attacks, as some sites were for instance closed to traffic from outside the country (Traynor, 2007). They were also prepared to the extent that the attacks did not manage to seriously threaten the national security of Estonia, although the private sector did suffer some economic damages (Reinart, 2009). As to the source, the attacks were traced to computers from all over the world, for instance China, Peru, Egypt and the US. Although there were thousands of attacks, Estonian officials claimed that they were quickly able to see that a large part of the attacks were coming from Russia, and even from Russian state institutions (Traynor, 2007). Many Estonians were quick to claim that the Kremlin was responsible, but Moscow responded with accusations towards Estonia and other former Soviet Union satellites for being quick to blame Russia for anything that happened (Traynor, 2007). Certainly the Russians looked suspicious, but as is often the case in cyber-matters, nothing could really be proven.

The cyber-attacks against Estonia lasted for about three weeks, coming in three distinctive waves. The first wave began on April 27th when the riots caused by the 'Unknown Soldier' started, lasting until May 3rd. The second wave came on May 8th and 9th, two important days in the Russian calendar, dating back to Second World War and the victory over Nazi Germany. That wave is also connected to a speech made by the then president of Russia, Vladimir Putin, where he publically attacked Estonia and compared the Bush administration to the Hitler regime. The last phase of attacks came a few days later, lasting for roughly a week (Traynor, 2007). The obvious linking theme is of course the connection to the Second World War and Russian history, i.e. a 'real world' theme that in this case just happened to be pursued with the cyber-weapon. The waves of cyber-attacks also had different features, the first being more the work of 'hacktivists' using rather amateurish methods, such as hacking into websites for the coalition parties and placing fake apology letters from the prime minister. The second phase was tougher to manage as a full-scale cyber-attack began, using botnets that

are estimated to have been composed of up to a million infected computers (Ruus, 2008), and causing traffic a thousand times heavier than usual on the Estonian websites. Hardly any website would be able to handle that traffic.

At the time of the attacks many of NATO's cyber-experts were at a conference in Seattle. Although cyber-attacks are not considered clear military attacks by NATO, and thus not evoking Article 5 of the North Atlantic Treaty, some of the cyber-experts were rushed to Tallinn to help defend the NATO member. The cyber-defence of Estonia was led by the director of Estonia's CERT (Computer-Emergency-Response-Team). He had been battling cyber-crimes for ten years before the attacks in 2007, but he also had a valuable asset. In Estonia there is a small network of information-technology experts from the private and public sector who are linked by friendship and could be called to help in the country's defence (Ruus, 2008). The closeness of the group resulted in quick sharing of information and received admiration from all over the world. Despite getting additional support from many other countries, however, the attacks could not be fully defended against. It was actually necessary to counter-attack in order to get the upper hand against the attackers and turn the tide around (Ruus, 2008).

In the end the casualties of the three-week onslaught were rather miniscule. The e-mail server for the Estonian parliament was unavailable for four days, the customers of the largest bank in Estonia were unable to access their accounts for a few hours and the main Estonian news agencies encountered disruptions, among other being forced to close their site to traffic originating from outside the country. For most of the sixty percent of Estonian people who use the Internet every day, very little changed and most people noticed nothing (Ruus, 2008). The fact that the attacks did not cause more damage than it did has also led to speculation regarding who the perpetrators actually were. For instance it has been stated that the Kremlin could have done much more damage if it were behind the attacks (Traynor, 2007). It can also be mentioned that Estonians, just like Kyrgyz and many other former Soviet bloc nations, have been fighting their past. A large attack that is thought to have originated from Russia should be able to convince many to look more to the West rather than to Russia. At all events, the Estonian episode caused a clear and sudden rise of awareness in the Western world about cyber-threats. NATO agreed to establish a Cooperative Cyber Defence Centre of

Excellence in Tallinn, and a year later seven NATO members – Estonia, Latvia, Lithuania, Slovakia, Spain, Germany and Italy signed an agreement formally setting up the Centre. The US takes part as an observer and any other NATO country is allowed to step in at later date (Goldirova, 2008). The question of whether NATO should have done more to defend Estonia directly, as the NATO charter states that an attack against one member state is an attack against them all, remains somewhat murky partly because there is little clear thinking over whether any cyber-attack can be seen as an act of 'war', as already noted above.

There are some aspects that make the attack on Estonia particularly interesting, and set it apart from other DDoS attacks. The scale and number of targets that were attacked were exceptional, adding to the theory that this was not a 'grass-root' attack, but rather required great planning. Also the duration of the attacks required extensive efforts, and could hardly have been sustained by a traditional criminal organization without substantial financial support. The facts that the state was attacked rather than single organizations or financial institutions, and that no attacks extended outside Estonia, add to the same impression (European Commission, 2009, pp. 74-75). All these clues point to an interesting conclusion. The motives for the attacks were not financial, but were rather ideological and/or state-centric. The level of planning and coordination needed to perform the attack would point towards state participation, although the start of the conflict was obviously because of ideological differences. All these features make it plausible to identify the RBN as a prime mover with complicity or even assistance from Russian state personnel (Blakely *et al*, 2007). As noted, the RBN were also implicated in Kyrgyzstan and will reappear in the Georgian case below.

3.2.4 Georgia

Both Estonia and Georgia were inside the former Soviet Union and both have been struggling with that legacy. Any such nation can be divided when it comes to whether the way of the future lies with Russia or the West - as the alternatives are often defined. Estonia has moved decisively into the West by becoming a member of the European Union and NATO, while Georgia is at an early stage on the same road - but a road chosen is a road halved. In August 2008, a conflict erupted that can be said to have been brewing for more than a decade over the status of the Georgian provinces South Ossetia and Abkhazia. The Russian army ended in

control of both and Moscow subsequently supported their declaration of independence (Gorman, 2009a). Russia has claimed to have been protecting the people of the provinces against genocide while Georgia portrays the incident as a Russian seizure of its sovereign territory (Wertsch and Karumidze, 2009).

The Georgian conflict was a major shock for the European security system but also has another claim to fame: it is believed that a cyber-attack was for the first time used in a real strategic manner against Georgia. The simultaneous attack greatly disrupted the capabilities of Georgia to communicate with the outside world. Over 20 websites were unavailable for more than a week, among them the sites of the Georgian president, the foreign minister, as well as the National Bank of Georgia and several major news media (Gorman, 2009a). During the attack the Internet access in Georgia was sporadic, as was cell phone reception. Russian troops aimed at means of communication, e.g. with the bombardment of cell phone towers (Thompson, 2008). While the latter may be considered regular procedure in times of war, the disruption of Internet possibilities has not been used to any real degree in the past (Gorman, 2009a).

The attacks on Georgia in August 2008 were traced to 10 websites registered in Russia and Turkey, and paid for with stolen credit card numbers from American and French individuals (Gorman, 2009a). These ten sites were then used to coordinate an elaborate attack against the Georgian sites, effectively disrupting most of them. Although the Georgians did not have a CERT team at the time of the attacks, there were still counter cyber-attacks aimed at Russia. It was reported that at least one Russian newspaper felt the attack on its servers (Vamosi, 2008).

The cyber-attacks against Georgia can be considered to have a high level of coordination. Reports about the attack claim that the cyber-campaign was developed some time before the actual attack. In a ‘traditional’ spontaneous cyber-attack, the attacked sites would be examined and chosen once the attack was underway. In the case of the Georgian cyber-attack, specific sites were attacked with pre-tailored software, indicating advance planning. At least three types of software were used to disrupt sites, using technology that is used to test how much traffic a site can handle. Another type of software makes the affected

sites exhaust their resources by trying to access non-existent sites, cutting out other traffic (Rutherford, 2009). Pictures that were used to deface Georgian sites had been prepared two years before the 2008 attack but not used previously (Weitz, 2009). Internet sites and domain names were set up with such speed that it is very unlikely that the target had not been analyzed before. Attack scripts had probably been written and even exercised before the actual attacks. When the actual fighting began, Russian social networking sites were used to spread suggested targets and means of attack that could be used even by people with very limited computer knowledge (Weitz, 2009). Reports claim that even though the actual perpetrators of the cyber-attack against Georgia were civilians, the coordination of the attacks must have at least been done in cooperation with the Russian authorities that would provide important information. This can for instance be seen in the fact that the cyber-campaign had started before the news media has reported that the actual physical conflict had begun (Weitz, 2009).

The fact that the damage caused by the cyber-attacks was not greater than it was has raised some questions: had a high level individual ordered that the damage be kept minimal? Disabling and defacing some websites can be considered minimal damage, given that the attackers also seem skilled enough to have been able to sabotage critical infrastructure, disrupting Georgian society even more. The military capacities of Russia are of course far more advanced than Georgia's, and therefore the results of the physical conflict were perhaps never in question. Perhaps Russia used the cyber-weapon more to win advantages regarding public perception, which might be manipulated for instance by depriving the other side of the capacity to make public what is happening. In that case it can be claimed that the nature of the cyber-attacks was perfectly compatible with the superior military power of the Russians (Weitz, 2009).

When the cyber-attacks had been going on for a few days, a new stream of spam was sent out regarding Georgia. The e-mails were badly spelled letters supposed to look like a news report from the BBC and aiming to arouse the curiosity of the reader, and remarkably, they amounted to around 5% of the total spam traffic at the time. If a reader were to click the link to the alleged BBC article, his/her computer would most likely become infected and would then be used in the next onslaught against Georgia (McMillan, 2008). This highlights

another difference between cyber-attacks and traditional military attack, in that the former can gain reinforcements without much effort and use them at once. A year after the attacks against Georgia, a lone Georgian computer user had been very critical of Moscow's attitude towards Georgia, and was thought to be planning some critical web-posts. The response of the Russian side was an attack against any possible media the Georgian could use, Facebook, Twitter, Youtube and blog site. The attack was so powerful that the effects were felt around the world and even took Twitter offline for some time (Weitz, 2009).

Experts have compared the attacks on Estonia and Georgia and estimated that there were more individual cyber-attacks, but considerably fewer computers, involved in the latter than the former case. This can be explained by the fact that Estonia was much better prepared for any type of attack or increased traffic than Georgia was. The threshold for what the Georgian servers were able to handle was much lower than the servers in Estonia (Rutherford, 2009).The Estonians were one of the first countries the Georgians contacted when the cyber-attack was underway, asking for help in the matter. The Estonians then put them in contact with international experts who were able to assist, and the Georgians were also able to move a few of their websites from Georgian sites onto either Estonian or American servers. These servers also had some trouble maintaining the service due to the increased traffic caused by the attacks (Rutherford, 2009).

It has been judged that Russia's cyber-capacities evolved after the conflict with Estonia in 2007. The Russians will certainly want to continue developing, especially if they want to be ready for conflict with nations bigger than Georgia (Weitz, 2009). If the Russians revealed some of the cards in their hands by the Estonian and Georgian attacks, other aspects of their capacity remain mysterious. As will be seen later in this chapter when Russia is examined, the country seems to have probed at least some other possible adversaries in preparation of a cyber-attack. Insofar as it was useful for the Russian authorities to have the Russian Business Network as a possible scapegoat, their return must be good news for Russia. Plausible deniability is a good thing when it comes to cyber-attacks, and the Russians have certainly used that. It should be mentioned that the RBN are thought to have been involved in the attack against Georgia.

A final lesson from Georgia may be that while the country temporarily lost some means of communication it was still physically part of the mainland of Europe, in touch with many neighbours. Information could still travel over the borders, if not at the expected modern speed. The situation would be drastically worse if a country was not only under attack by a larger country that successfully used cyber-attacks to disable its main ways of communication, but was also an island in the middle of the North Atlantic Ocean. That would certainly make the situation more difficult for everyone involved.

3.3 Nations using Cyber-attacks

Over a hundred states are working on the capacity to use cyber-weapons to cause damage to other states, according to reports by the McAfee computer security company (Council of Europe, 2008, p. 44). Representatives from security agencies have said they have had to reroute government agents from the usual tasks to cyber-threats. Chinese and Russian cyber-warriors are said to be the main offenders, although this is hard to prove, as will be seen below (Council of Europe, 2008, p. 44). While the Internet was invented and implemented during the Cold War, it seems to have outlived its inventor and to have gained the potential to create a Cyber-Cold War today (Williams, 2007). At first there were mostly probes, where the integrity of the system is measured. That has evolved into full scale attacks, although short-lived, where defence information is sought through any available system. Now it seems that intelligence agencies all around the world are actively using the Internet as a tool to gain information about other nations, whether adversaries or not (Williams, 2007).

Reports say that Russia and China are in the forefront in the use of cyber-attacks (Tully, 2009). American defence institutions have been taking more notice of Chinese and Russian activity on the Internet, as well as activities from other entities, including non-state actors, violent extremist groups, cyber intruders and criminal organizations. These entities are seen as undermining American interests in a growing way and thus deserving the attention of the American government. The recommendation in the case of cyber-attacks on American infrastructure was that allied intelligence services, industry and academia in the field of intelligence technology be extended so that American infrastructure could be protected. It should be mentioned, and as will be pointed out in the US section, that the US is

often quick to point to the threats that the Internet can pose, but that does not mean that the US is not also actively using the same methods.

In the Middle East a cyber-war has been going on for a long time. The Israel-Arab conflict has been fought online to a great extent, with both sides hacking into each others' websites, defacing the sites and putting up propaganda and other material. For instance a group of Moroccan hackers have been actively defacing Israeli websites for many years, while other groups have for instance infiltrated and taken down an Israel radio station. These attacks are not state-governed by themselves, and can be considered low-hanging attacks, meaning that the targets are often rather easy targets (Jenik, 2009).

Although it was previously stated that the nature of cyber-attacks between states had altered from simple probes to full scale attacks, there are still some further aspects that need to be examined. States are to a greater extent placing software into the systems of other countries, without the knowledge of the hosting state. The reason the hosting state does not know about this foreign software is that the software in fact does nothing until it is activated. It has been reported that cyber-spies from Russia and China have placed software for instance in the electricity system of the US. The system is of course still functional, but it is estimated that in times of a conflict the software could be activated and the electricity system be brought down (Gorman, 2009b). The mapping of the electricity system and other critical infrastructure is an important aspect of any pre-war planning. That is not to say that Russia or China are planning a war against the US, but rather that the two nations want to have done their homework in case of a conflict. Such control of vital internal functions could give China and Russia possibilities to pressurize and blackmail the US if the need came. China might prefer this approach to a direct physical attack as the Chinese have great financial interest in the US. When asked about such possibilities the Russian authorities reject all claims of cyber-attacks, and deny any attacks or hacks of any kind. The Chinese also reject these claims and mention that China has strict laws against cyber-attacks and is participating in international cooperation against infiltration of critical infrastructure (Gorman, 2009b).

If there is any truth in China and Russia condoning or at least planning such attacks it may be assumed that other countries have thought about them, not excluding the US itself (see below). Even if the cyber-aspect of war has not been prominent in the past, it could become a vast part of modern conflict in the near future. The Georgian conflict introduced cyber-attacks as a part of 'traditional' conflict, but in the case of a conflict between the greater nations of the world, cyber-attacks and attacks on critical infrastructure could very well become an even greater part, or even present the greatest part of the conflict. At that time the possibility of a conflict without casualties could even present itself.

3.3.1 Russia

Russia presents an interesting profile when it comes to cyber-matters, as it can be said to figure on both sides of the equation. Like any other country, Russia has been the victim of cyber-crimes. Internal struggles have been fought online as well as in the real world. But Russia has also been suspected to have been using cyber-weapons against other countries. The two biggest and most commonly known cyber-attacks of later years, Estonia and Georgia, have both been traced back to Russia in some way. And although Russia may not have fully evolved its cyber-capacity it is certainly giving cyber-weapons a place in its arsenal. The internal disputes that Russia has had over the years are of course a problem for Russia, but also offer possibilities when it comes to plausible deniability.

Nationalism and a strong idea of history seem to have been in the background of the attacks that have been traced back to Russia, and may offer a general clue to the Russian modus operandi. In 2009 a failed attempt at a cyber-attack against Poland was reported, which was also believed to have originated in Russia and coincided with the anniversary of the start of the Second World War. Prime Minister Putin was visiting Poland at the time of the attacks, which may also point to a connection (Leyden, 2009b). The anniversary of the 1939 invasion of Poland by Germany and the Soviet Union might logically cause Polish hackers to attack Russia instead of vice-versa, but Russian cyber-attackers have not needed much provocation for attack in recent years. Of course it should be mentioned that Russia has perhaps become something of a convenient scapegoat when it comes to cyber-attacks, though the obscurity of Russian behaviour itself opens the way for such suspicions. The Georgian cyber-attacks showed that the

capabilities of Russia when it comes to cyber-attacks are certainly evolving, but also that there is a long way to go, given that the Russians were behind the attacks against Georgia (Weitz, 2009).

The law environment in Russia has also been a cause for concern when it comes to the battle against cyber-criminals. As was seen in chapter 4.1.2, the RBN were allowed to operate in Russia for quite some time before they moved to China. The RBN was beneficial for the Russian authorities, just as the lax view of the Russian authorities is beneficial for any cyber-criminal living in Russia. As noted, international law-enforcement have had to go to great lengths in order to apprehend Russian cyber-criminals, and the few victories the FBI has had in apprehending Russian cyber-criminals have involved luring them out of Russia to the US with a hoax of some kind (Bronk, 2010). Russia has neither been willing to allow international law enforcement to enter Russia in pursuit of Russian criminals, nor to expatriate the criminals to other countries. This has encouraged the theories reported in this thesis that the Russian authorities are profiting too much from these Russian cyber-criminals to be willing to rid themselves of them quite yet.

3.3.2 China

China is a particularly complex case to handle when it comes to cyber-crimes and cyber-warfare. The Chinese government has some high-profile disputes that it would categorize itself as internal, notably its policies against Falun Gong and in Tibet. The point here is not to judge those issues but to note that they have, among others, also been fought out in cyber-space – as will be discussed below. There is also the question of the restrictions that the Chinese government has tried to apply to its citizens' access to the Internet and online services, and the international disputes that have followed. The size of the Chinese market makes the stakes very high for any companies affected by such cases.

Inter-state altercations involving China have also been followed by cyber-attacks. For example in 2001 a US airplane hit a Chinese fighter plane, resulting in the death of the Chinese pilot. This resulted in a sustained campaign against American computer networks, though thought to be the work of independent Chinese hackers, not acting on behalf of the Chinese government. The fact that

Chinese hackers have received international attention could make it easier for the Chinese government to blame these hackers if any attacks were to be traced to China. As seen in the case of Russia, this can be a valuable asset.

Even though China may be very advanced when it comes to using cyber-weapons to fight its battles, a large part of China could still be considered a developing nation. A certain symptom of development is that computer owners don't necessarily want to pay for defences for their computers, thus leaving them vulnerable to be infected and perhaps even used in botnets.[14] The Chinese government has closed down training sites operating in China where thousands of people, often young men, have received training in tasks such as stealing accounts and writing and using Trojan viruses (Branigan, 2010). The student fees are small but with thousands of members, this small fee quickly amounts to millions of Yuan.

China has taken a very peculiar approach when it comes to Internet access for its people. In 2009 the Ministry of Industry and Information Technology announced that it would make certain software mandatory in all computers sold in China, whether manufactured domestically or imported, to make it impossible for people to search for unsuitable material (Bristow, 2009). Definitions of what is considered unsuitable would be placed at the discretion of the government. Official statements indicate that material such as violence and pornography will be restricted, as this can be harmful, especially for young people. Because of China's earlier attempts to restrict access to politically sensitive material, critics are suspicious that the Chinese government will also use this new software to block access to those kinds of information (Bristow, 2009).

Strong as the criticisms of China's cyber-policies have been, the Chinese have also strongly defended themselves: the question is whether the answers should be considered satisfactory. The arguments regarding Google are addressed later in this chapter. The Chinese authorities have justified the restrictions on individual Web access as being in the people's own interest, citing e.g. the recent protests in Iran where social sites like Twitter (a large real-time communication

[14] Stolen copies of Windows can also be very influential when it comes to the spread of viruses and trojans.

website) were widely used and China suspects the US of having instigated this (LaFraniere and Ansfield, 2010). China has accordingly blocked most of the popular social sites, originating in the West, on its own territory. It seems clear that China is worried about losing power over its people, and a typical example was when the authorities imposed a virtual communications blackout on the province of Xinjiang, restricting text-messages, international phone calls and Internet access to all but a few government-controlled websites. These restrictions applied to roughly nineteen million people, and were in effect for six months (LaFraniere and Ansfield 2010). The damage and disruption caused are undisputed.

Hacking can, to a great extent, be called a grass-roots movement in China. The 1999 bombings of the Chinese embassy in Belgrade caused great anger among ordinary Chinese. While many were throwing rocks at the US embassy in China, others were planning cyber-attacks against the US. This bred up a large generation of highly trained computer hackers who are now being recruited into the Chinese army, according to reports (Areddy, 2010). Although China differs from Russia in the respect that China seems to have rather strict laws regarding cyber-crimes, they also seem to use the works of hackers for the benefit of the state. The Chinese online environment offers easy access for beginners, where for instance the making of a virus is handled by an ‘assembly-line’ procedure, with many hands making the job easier, and the makers also sharing the proceeds to some extent (Areddy, 2010). This would certainly make it easy for young Chinese people to get into the business of hacking, providing more people for the official cyber-army to recruit.

The People’s Liberation Army (PLA) is said to have been developing the cyber-aspect of its strategy for some time, but it was not until after 2000 that its cyber-division started to draw attention from other nations, for example the Department of Defence of the US (Lemon, 2007). The PLA has been training extensively against a possible computer attack in the last years, but also working on counter-attacks, for instance by working on their virus-making capabilities (Lemon, 2007). The PLA are also said to have been making small attacks on foreign countries for the last years. Chinese attackers are said to have attacked the British Foreign Office, the House of Commons, and are even thought to have

hacked in to the US's Pentagon. That attack was considered to be the most successful cyber-attack to date on the US defence department (Norton-Taylor, 2007). This is said to be part of a technique that is called 'pressure point warfare' – meaning the use of special nodes that can leave the adversary paralyzed. The infiltration of critical infrastructure to leave behind software that can effectively disrupt the infrastructure would be an example.

Although the Chinese government denies any involvement in cyber-attacks against other states, the evidence seems to point to the contrary. The PLA has been active in recruitment for its cyber-militia, even going so far as to advertising in Chinese newspapers, asking for the most capable hackers of the country. These advertisements offer cash rewards and further advancement for the most capable. The PLA is even thought to be paying smaller hacker groups a small stipend so that they can continue to progress (Elegant, 2007).

Undocumented aid for hacker units is just one of the things making cyber-attacks hard to handle for the international community. Some nations are clearly exploiting the anonymity of the Internet, the possibility to fight through proxies, and the resulting deniability, while the victims find it hard to press home accusations or to justify reprisals. This is something that the Chinese have benefitted greatly from (Elegant, 2009). The threshold for what nations will tolerate seems to be quite high when it comes to cyber-attacks. Cyber-attacks against Germany are said to amount to billions of Euros each year, but all they have elicited is a public statement where that Chinese are blamed, with no real punishments being meted out. Along with placing software into foreign systems, the Chinese are also said to be stealing technology that will allow them to become the economic leaders of the world by 2020, and cyber-espionage offers them a particularly cheap method (Connolly, 2009). On any other occasion espionage and theft of this magnitude would cause an international conflict, but apparently not in this case. While the difficulty of proof is certainly a factor, the size and daunting power of the nations thought most responsible may also be significant. If the guilty parties were for instance in Iceland, it can be assumed that they would be chased down and the government of Iceland would no doubt be blamed for allowing the crimes to be perpetrated. In this case size really does matter.

3.3.2.1 China vs. Google or 'Operation Aurora'

By the end of 2009 the Chinese Google site was under significant cyber-attacks. The relationship between China and Google has been strained since it began in 2006, when Google agreed to China's censorship terms in order to be allowed to operate in China. As has been mentioned, the Chinese authorities are especially keen to suppress both external and internal discussion of certain matters, such as the events at Tiananmen Square in 1989 and the fate of a number of minority groups all around China. The Chinese government has been unwilling to allow its citizens to gain full access to information about these events, and because of the size of the Chinese market it can force incoming companies to agree to their terms. Nations that have business interests in China have even been unwilling to mention these events and other humanitarian issues in China in fear of retaliation from the Chinese government.

In the years since the launch of the Chinese Google site, Google.cn, the public-private relationship has had both highs and lows, with the Chinese government increasing their claims to restrict free-speech. But in the beginning of 2010, Google announced that there had been extensive hacking attempts that were traced to China, where the targets of the attacks were the email accounts of known human-rights groups. The attacks have been called 'Operation Aurora', the name thought to be used by the attackers. The severity of the attacks has been said to have been significant, as they were both widespread and sophisticated (Zetter, 2010a). As one of the best known sites of the world, Google is under constant cyber-attacks, most often by novice hackers or 'script kiddies' but these attacks mostly go unannounced by Google. It can then be assumed that when attacks are announced, they are of a more serious nature. In the Chinese case Goggle announced that the site would be ceasing all restrictions on individual searches on the Chinese site, knowing that the move would probably lead to the closure of the site (Zetter, 2010b).

The matter then turned into a battle of sorts between the US and China. Google has enlisted the aid of the National Security Agency, NSA, to help them against the cyber-attacks (Zetter, 2010c). The deal allows Google to share information with the NSA in order to be better able to defend against possible threats. This has caused some controversy, as there is fear that the NSA would try

to misuse its situation to gain information about the searches and email content of Google's customers (Zetter, 2010c). The NSA is famous for spying on Americans, supposedly for their own good: for instance during the Cold War it worked with Western Union to read telegrams sent within the US, and under the cloak of the war on terror it has been eavesdropping on customers calls and Internet traffic (Shachtman, 2010). Whoever may be in the right over the Google incident, the issue of governments using cyber-techniques to intrude on their citizens thus arises on both sides. While cooperation between the public and private sector to best fight a common threat would often be recommended, this can hardly be thought to be the best example of that cooperation.

The public discourse regarding cyber-threats has actively made the Chinese look to be the villains of the world, with the Russians claiming second place. The truth would seem to be that the discourse is too West-oriented in this matter, as in many other aspects of security studies. Criticism of China and Russia draws attention away from Western nations like the US, Israel and France, who can also be called cyber-attackers. These nations are of course only the tip of the proverbial cyber-iceberg, where the matter comes murkier the deeper you go. It has been estimated that over one hundred countries all around the world are working on their cyber-capabilities. That could very well be an accurate estimate, as it is much easier for a relatively small country to develop powerful cyber-weapons than in the case of conventional arms.

The dispute between Google and China has also had some other international repercussions, as Secretary of State Hilary Clinton has used opportunities following the attacks on Google to call for international agreements regarding cyber-weapons. She argued that all states were vulnerable to such attacks and states resorting to cyber-weapons should be made to take the consequences of their actions (Goldsmith, 2010).

In February 2010 it was announced that US specialists believe they have identified the person responsible for the attack against Google. Specialists traced the attack to two computers placed in educational institutions in China that have some connections to the Chinese military. However, the computers' owner was not necessarily the true attacker as the computers could have been compromised

and exploited as a smoke-screen for the real culprits (Menn, 2010). This highlights another difficulty: while it is on the face of it good news when a single individual or group can be found to blame for attacks, such individuals could always be the victims of a set-up by more powerful forces trying to evade an international dispute.

3.3.3 Israel

Israel would be considered a small nation on the larger world scale but has had more than its share of disputes, both with its neighbours and others. It comes then as no surprise that Israel has been working on its cyber-capabilities and since its 2006 war against Hezbollah, has successfully been making cyber-attacks a part of its 'traditional' warfare. For instance in 2007, Israeli jets destroyed a nuclear facility that was being built in Syria. Evidence seems to indicate that Israeli cyber-warriors hacked Syrian radars and other ground level defence units, disabling them and thus giving the jets enough time to get to their targets and launch the strike without much resistance (Eshel, 2010). Syria is of course only one of Israel's many enemies in the Middle East. Another is Iran, which has been working on its nuclear program. Despite Tehran's promises of peaceful ambitions regarding enrichment of uranium, Israel is said to be working on cyber-attacks against Iran's nuclear capacities. That could be seen as the only viable approach, since a traditional military strike would have no guarantees of success and could unleash retaliation at a time when the US, Israel's greatest supporter, has its military hands full and might be unable or unwilling to help (Eshel, 2010). The Israeli cyber-warriors are said to have attempted to place malware within the Iran nuclear system, but the results are yet to be revealed - and may never be, as Iran is unlikely to admit having succumbed to cyber-attacks and Israel would want to conceal its responsibility and true capacities. After the report of such an attack the Israeli government indeed imposed a news blackout, with its usual no-comment stance (Urquhart, 2007). This tactic is typical of other suspected cyber-capable nations, but Israel's small size and experience may help it to successfully keep its cyber-capabilities hidden.

3.3.4 The United States of America

Although the US has been named as the victim in many of the reports mentioned in this thesis, it can be assumed that the cyber-capabilities of the US are equally as

great, if not more than most of the countries mentioned. Aggressive use of such capacities by the US would not necessarily be more legal or better justified than when done by Russia or China. While progress in US cyber-defences was slow after Richard Clarke's warnings reported from 2002, in 2009 there are signs of the issue becoming a big one. It certainly seems as though the administration of Barack Obama intends to make the matter a high priority. In February 2010, Denis Blair, the Director of National Intelligence, gave a statement about the threats facing the US, and cyber-threats were the first threat he named. Mentioning vulnerabilities such as that of critical infrastructure, Blair argues that the matter should best be handled by a cooperative effort by the state, the private sector, and international allies (Blair, 2010).[15] While the US authorities are very open about their efforts to strengthen cyber-defences and vocal about any attack committed against an American company within the US or even on foreign soil - for instance with the cyber-attack against Google – they are giving much less away about their offensive capabilities (Kingsbury and Mulrine, 2009). This is not unusual in US practice but underlines the difficulties discussed in the theoretical chapter above about achieving any kind of cyber-deterrence.

One of the ways the US has been working to become ready for a full-scale cyber-attack is by setting up war simulations that are designed to test the responses of the defence sector. This was done in the beginning of 2010, where a large scale incident was simulated. A virus was distributed through an iPhone application, which then led to the disabling of the cell phone network and Internet access and ended with most of the East Coast being out of power because of a failure in the electricity grid (Neal, 2010). The simulation allegedly failed completely, displaying that the US was nowhere near ready for a large-scale incident. The private sector, public sector and regular individuals failed to act according to the threat, revealing a number of vulnerabilities. One vulnerability that emerged is that people in the US are not quite scared enough in such a case to let a government official tell them what to do. Another is that the private sector was unwilling to cooperate with the government in order to try to contain the problem, for instance by cutting off Internet or cell phone service. Finally they found out that the government is too busy and lacking in spare capacity to

[15] Report available at URL: http://www.dni.gov/testimonies/20100203_testimony.pdf

successfully deal with an incident of this scale (Neal, 2010). While it is apparent that the simulation was a failure, it is of course better that the short-comings of the actors in the US system are clear before there is an actual incident, and in that respect, the position of the US has improved with the simulation.

The US State Department has been pushing for openness and cooperation when it comes to cyber-problems and might wish to promote international agreements regarding the use of cyber-weapons, but this would probably run into difficulties notably with Russia and China. While an international code might be achievable against cyber-crimes performed by individuals, providing for jurisdictional cooperation and so on, it would hardly be able to stop state-sponsored cyber-crimes (Bronk, 2009). An international agreement that could aid in the apprehension of cyber-criminals is certainly a good thing, and if the new direction of the Obama administration is able to make such an agreement a reality, that could be welcomed. International efforts will be examined further later in the thesis. The US is highly ranked when it comes to Internet access, and where access is high, it can often be assumed that infected computers are also many. Thus many cyber-attacks could be actually coming from the US, even though the perpetrators are situated somewhere else. The cost of making all these infected computer secure would most likely be passed down from state to private sector all the way down the individual user who is unlikely to want to pay.

While the US might be fighting on many fronts today, one of the oldest adversaries is the terrorist group Al-Qaida. Although they have been using the Internet for recruitment purposes, the impact of Internet attacks is probably still too limited for Al-Qaida, since they are more interested in causing direct impact and terror by blowing things up and killing infidels (Bronk, 2009). There are rumours that the NSA has the technology to hack into computers of Al-Qaida members where information can be examined or deleted, but this of course cannot be verified. It has also been mentioned that the US has contemplated using cyber-weapons, for instance during the later invasion of Iraq. A strategy was developed to use cyber-attacks against the financial market in Iraq, but that plan was abandoned because the US planners were not sure about the results, or whether they could be maintained (Kingsbury and Mulrine, 2009). There are many thoughts that follow that story, for instance that if true, the US could be the only

country so far to hold back from use of a cyber- weapon because the results could not be completely foreseen. The story also serves, however, to underpin the idea that the offensive cyber-arsenal of the US exists and presumably is being steadily strengthened.

Then there is also the fact that there are many ‘hacktivists’ in the US, just as in most other countries, many of them attacking oppressive regimes and groups all around the world. These individuals in some cases even have sponsorships from institutions (Goldsmith, 2010). Lastly, the US is known to have a great number of cyber-warriors placed all around the world under control of the NSA, who could launch attacks without making the US seem involved - very similar to the tactics the Chinese government has been using and the US Secretary of State has been critiquing. For the US not only to give up but eliminate the possibility of such operations would certainly be costly and therefore somewhat unlikely, and the same might be said of any other nation that uses cyber-warfare. This makes it seem unlikely that leading nations would press through an effective international agreement against cyber-weapons, and a strong draft is perhaps more likely to come from an NGO or an institution of another nature. This matter will be looked at further in later chapters.

4 Iceland

It has been noted above that one of the first cuts made in times of recession is spending on computer defences. But it has also been remarked that cyber-crimes flourish in times of recession, as they carry little or no added cost: all a criminal really needs is a computer and an Internet connection, which can be found at a local cafe. The battle is already skewed against the law-abiding individual, who has limited abilities to fight against an adversary with far greater numbers.

In this chapter we will turn our focus to Iceland. We will try to determine what the weaknesses and strengths of the country are when it comes to cyber-defences and critical infrastructure. This will be done by looking at the available information, starting with the recently published Threat Assessment where a wide range of hazards for Icelandic society is examined and evaluated (Foreign Ministry of Iceland, 2009). More specific vulnerabilities will be discussed with the help both of published studies and targeted research interviews carried out with Icelandic individuals with knowledge of the subject, who were asked if they considered Iceland to be vulnerable to cyber-hazards and what action they would recommend. For example, is the fact that Iceland has only a small number of Internet Service Providers (ISP) a weakness or strength when it comes to vulnerabilities? Is Iceland's small group of cyber-experts a benefit for Iceland, and how could they be used better? Is Iceland's island status a pro or a con when it comes to security matters? Turning to possible solutions, the first official study of a possible CERT/CSIRT team being established in Iceland will be reviewed together with the expert comments made on it during consultation. The chapter ends with a more general discussion of how Iceland needs to and could organize its cyber-defences in future, including the interface with international efforts.

4.1 The case of Iceland: Cyber-security and Critical Infrastructure Protection

In terms of national reliance on the Internet Iceland has been ahead of the other Nordic states, although all of them are very advanced. Among Icelandic people

between the ages of 16 and 74, 88% claimed to use the Internet at least once a week. The lowest percentage in the study was in Finland, where only 78% of people in the same age group claimed they used the Internet weekly (Nordic Council of Ministers, 2009, p. 13). Although this of course tells nothing about how much people may rely on the Internet for practical functions, it can be used as an indicator that a great part of the Icelandic people are computer-literate. It also underlines that the Nordic states have very similar profiles that should lend themselves to similar solutions. Another feature shared with most Nordic states is the long lines of communication that are needed to link the countries' sparse populations, with the resulting issues of infrastructure reliability and protection.

The first part of this section uses the 2009 Threat Assessment report as a basis to analyse possible threats and risks both to Iceland's cyber-systems as such, and to the broader infrastructures on which they depend. It then goes on to look for specific vulnerabilities linked with e-governance, commerce, and so forth, and ends with some recent concrete examples of how accidental or intentional damage could occur.

4.1.1 Threat Assessment for Iceland

The only real step that Iceland has taken towards systematically assessing what threats the country may face was the appointment of an independent Threat Assessment team that presented its report in March 2009 (Foreign Ministry of Iceland, 2009). The assessment was led by Valur Ingimundarson, a noted historian and lecturer, at the behest of the former Minister of Foreign Affairs for Iceland, Ingibjörg Sólrún Gísladóttir. The banking crisis erupting in the fall of 2008 clearly overshadowed the findings of the assessment, adding a further revelation about the nature of the Icelandic system and its vulnerabilities.

Iceland's position has long been a peculiar one, being a member of NATO without ever having an army of its own. For a long time the country relied on the protection of the US armed forces stationed at Keflavík. Now that the US has moved away the time has come for Iceland to shoulder more responsibility regarding its own defence, and to have a minimum capacity to cooperate with other NATO members, according to the assessment (p. 127). Because Iceland is not seen as facing any clear military threats from other states in the short or

medium term (p. 126), it is recommended that Iceland should focus its own efforts upon non-military factors rather than traditional territorial defence. These include civil security and infrastructure protection (p. 127).

In terms of cyber-security and the protection of critical infrastructure, the threats identified in the assessment report include natural threats, organized crime to some extent, ideologically motivated groups to a small extent and other threats to civil security. When it comes to natural threats, the most applicable are volcanic eruptions, earthquakes, floods and so on. While contingency plans are in place to respond to these types of disasters, these occurrences can affect the infrastructure of the country to a great degree (p. 128), damaging for example roads and bridges – though these have done relatively well in withstanding earthquakes (p. 132). Although Iceland is not considered to be a prime target for terrorist attacks, positions taken by the Icelandic government on international issues can raise that risk, making Iceland a possible target. While the main threat to air safety is considered to be terrorist attacks, they are still considered extremely unlikely (p. 132). Attacks against Iceland or other Nordic countries are not thought to be likely from international terrorist groups like Al Qaida but rather from extremist Islamist youth groups, for instance second- generation Europeans, who feel that they have not been fully accepted by their respective societies and could be radicalized under influence from international terrorist groups. The report sees fair and balanced immigration and refugee policies as the best way to prevent the risk of such groups gaining a foothold in Iceland (p. 128-129). While immigration and refugee policies have been working well for the most part in recent years, the worsening employment status in Iceland following the crisis could change that. There have been examples of racism and xenophobia in Iceland in the last few years, and social exclusion and alienation among foreign residents could increase those occurrences, adding to the risk of disaffected youth groups forming (p. 131). Some Icelandic organized crime groups have been cooperating with foreign crime groups, while other move into competition with each other. While some groups start in drug trafficking, they are likely to move into other fields such as extortion and money laundering. It is considered likely that the economic crisis in Iceland will stimulate the growth of the ‘underground economy’ in the short term (p. 130).

Iceland is highly dependent on imports of food and other goods, for instance oil to make diesel fuel for its fishing industry. The financial crisis revealed that Iceland can be very vulnerable when it comes to interruptions of supply. It can then be assumed that failure in communications could have similarly severe repercussions. Massive failure in the electrical system could also make food storage difficult (pp. 132-133). Iceland differs greatly from other countries when it comes to electricity, as around 70% of the energy used in Iceland comes from renewable energy, while the other 30 % are mostly used to fuel cars and the fishing fleet. Iceland's electricity system is not connected to any other state, and is thus not subject to any kind of 'domino effect' after a breakdown elsewhere such as has been seen in other countries; but that also means that there are fewer backup options in case of disruptions. The power system is still thought to be quite vulnerable, both to sabotage and natural disasters. There are no clear examples yet of the electricity system being targeted for sabotage[16] (p. 133). Even so, Iceland is very sparsely populated country and the communications infrastructure of the country is spread over areas that are not defended in any way. The communications system is rather simple and a limited number of actors oversee the entire network. While the network is circular in order to minimize disruptions, accidents or sabotage can cause malfunctions. Natural disasters have been known to cause nation-wide disruptions, as well as human error. The tapping of communications systems has been thought to be relatively easy, while the tapping of mobile phones would be more difficult but certainly not impossible (pp. 133-134). The report concludes that efforts should be made to protect the security of all Iceland's critical infrastructures and public utilities, including the fibre-optic cable system and the electrical grid, against all contingencies; and that the plans should include both emergency protection for existing systems and the development of alternative systems to function in the case of damaging incidents (p. 136).

Iceland has not so far been a target of a cyber-attack, although the possibility of such an attack can of course never be ruled out completely. The Threat Assessment discerns a number of cyber-weaknesses in areas integral to

[16] As has been mentioned earlier in this thesis, there is a possibility to infiltrate a system without the knowledge of the systems user, and that infiltration might be used at a later date.

Icelandic governance: for instance the official websites of ministries or sites used for elections could be subject to attacks. Iceland could also be victim to cyber-criminals breaking into electronic bank systems, although measures have been taken to guard against such occurrences. The fibre optic cable that circles the country is not considered fully protected and could be vulnerable to sabotage and natural disasters (pp. 130-131).

As a larger problem, because of the banking crisis the public debt in Iceland has skyrocketed, making it even harder to find funding for security and defence measures in the coming years. It is more important now than ever that Icelandic security organizations pool their resources to meet any new challenges that might occur (p. 124). Although the banking crisis did not bring the country quite down to its knees, it did show that Icelandic society is quite vulnerable to systematic breakdowns, and provides a warning to guard better against such contingencies in future (p. 125).

The recommendations of the Threat Assessment include several points where cooperation between public and private authorities is seen as especially vital, such as food security (p. 134), but also including more traditional threats that could affect cyber-security and other infrastructures where the private sector has a key role. Specifically, the report recommends that a CSIRT (Computer Incident Security and Response Team) team be established in Iceland – as has been done already in many other states - to handle the task of monitoring and to prepare and execute counter-measures against cyber-threats and attacks (p. 136). This team would not only respond to actual threats but also handle the education both of the government and the public in cyber-security (pp. 130-131), and channel Iceland's participation in international efforts to counter cyber-attacks (p. 136). The report sees the timely provision of information and advice to the public as being essential, in this field and others, to avoid the kind of panic responses that occurred at some points in the banking crisis and which are harmful for societal security (p. 138). The steps actually taken so far on the establishment of a CSIRT team will be reviewed further later in this chapter, but also in the next chapter when international efforts are examined.

The Threat Assessment report confirms that cooperation in cyber-security should be carried on with the Nordic countries – who are Iceland's closest partners and similar to it in cyber-profile - but also with other external partners when appropriate (p. 135). The European Union has developed strong cooperation in various fields such as organized crime, natural disasters and terrorism, and the report advises that Iceland strengthen its own cooperation with the EU in fields of shared concern. The EU also has standards and practices when it comes to setting up emergency response teams which can be taken into consideration when Iceland undertakes that task (p. 135). In sum, the Threat Assessment report stresses that cooperation between public and private actors within Iceland should be bolstered under an all-risks approach, but also that Iceland should work extensively with foreign organizations and states to counter both threats that might affect only Iceland and events that would be considered 'cross-border'. Recommendations of this sort will be seen again when the Stoltenberg report is presented in section 5.1.

4.1.2 Icelandic vulnerabilities and expert views

As was discussed in the securitization section of chapter 2, a highly relevant question regarding security is who is allowed to identify and categorize a given danger and indeed to decide what should be done about that threat. In the case of Iceland, since a formal national policy is still at a preliminary stage it is possible and relevant to ask all possible qualified individuals about the possible threats and how they should be met. This section aims to build a clear image about the threats that face Icelandic society, by looking at the work that has already been done by state officials but also what individuals in important sectors have to say about that work. These comments can be taken as pointing in a particular direction but do not necessarily offer the correct or only possible conclusions. It will be shown that most experts would agree that Iceland is vulnerable in many respects, but they differ more regarding the way that this danger should be met. There are still certain 'safe-haven' solutions that seem more fitting than others, and will be presented later in this chapter.

4.1.2.1 Iceland and 'e-Governance'

In 2007 the Icelandic government decided to launch a special project with the goal of making Iceland a leading nation in electronic services and governance through utilization of information technology. This project was called 'Iceland the e-

nation’ and was supposed to run from 2008 to 2012 (The Prime Minister's Office, 2008). It was based on three pillars: Service, Efficiency and Progress, and revolved around making information about official services available through a single website so that waiting lines would soon become obsolete. In recent studies Iceland has been judged as performing poorly when it comes to access to public services online and also in the possibilities for the public to be heard when it comes to matters of national concern. The actual administration of services is however considered good, and – as noted - public access and usage of the Internet is very advanced. It can then be assumed that if the possibilities for more self-service through the net were available, the people would make use of them. Instead of having to move from one office to another, they could access information from all these sources through a single portal. It would also be possible to handle all personal payments to the government through this portal, and this would also reduce administrative burden and cost with increased efficiency. This would also make it less important for people to live near particular locations, as more possibilities would be available online.

Iceland’s leadership as an e-nation would be based on its active democracy, its education and powerful industries. Democratic participation would be increased through more options for citizens to exercise influence within public bodies and in municipal elections. Education would benefit from added opportunities and availability of information. Industry would benefit from increased outsourcing as improved competitive conditions would make Icelandic companies more fit to survive on the international scene.

A large part of the e-Nation project is based on a single website, island.is, acting as a portal for the public so that all information can be accessed at a single place. The site was launched in 2007 and was designed as an information source, an interconnecting service and an individual-based service portal (The Prime Minister's Office, n.d). Information on all local authorities and institutions is available, and most of the public forms and applications that can openly be accessed anywhere online can now be accessed through island.is. The US has already developed a similar site, USA.gov, which has been judged as an excellent site providing extensive information and further links that citizens might need. It has been used as a model for other states, for instance some Nordic states, and

Germany has also been working on advancing its use of electronic governance, so that e-governance could become a force within the EU before long (Arnþórsson, 2010).

When it comes to Iceland's qualifications to handle this type of project, it seems that the country is well proficient. Many institutions in Iceland have IT systems that work well to handle their respective tasks. In 2005 a report stated that Icelandic institutions were far more advanced than Danish institutions when it came to using high technology (Arnþórsson, 2010). The main problem foreseen in connecting the Icelandic institutions in real life is that there has been no centralization among the operating systems, so that different institutions have different systems that might not be applicable with other systems without significant work. This can no doubt be remedied, but could require time and money. The integration and connections between ministries and institutions that would happen with portals such as island.is would reduce barriers not just between the public and government but also between ministries and agencies. Tasks could more easily be shared between the latter and the risks of duplication and of a particular task being lost on the desk of some official would be reduced. In the case of Iceland the smallness of the country and the infrastructure should make integration a beneficial solution, as there is plenty of information available and only the means to connect it are limited. But for such integration to take place, buy-in would be needed from the officials themselves and the question is why they should accept the disciplines involved, especially if there have never really been such 'checks and balances' as is the case in Iceland (Arnþórsson, 2010).

Projects such as this are developed for several reasons, but the main reasons in Iceland's case could be said to be the lowering of cost and the shortening of the democratic deficit. It is clear that when information is put at the fingertips of the people some operating costs can be saved. It is also clear that a single portal for people to voice their opinions as well as to receive information from their representatives or state employees will shorten the so-called democratic deficit. Insofar as a lack of information can have a prejudicial effect on people's lives, an information portal such as the one described here is clearly a good thing. Yet the dangers of this type of centralization are real, not only because of the vulnerability of a single site as target, but also because a single portal creates a

single large accumulation of personal details and a single place where the government could eavesdrop on its citizens (Arnþórsson, 2010).

As can be seen in section 2.3.2 on risk, the more that a particular item or service is depended on, the more risk is involved. An Icelandic ambition to become a leader in electronic services is bound to bring substantial risks, alongside the rewards that the policy predicts. In the case of the e-Nation project, making all these services available through this single website would increase the risk of them all being infiltrated or disrupted. If the website should be used as a portal for elections or matters of similar importance that would mean that a single target could be attacked if there was a will to disrupt the elections. The obverse point is that if there is a single site that can be attacked, only one site needs to be defended, while if the process was distributed over many sites they would all need to be protected.

The island.is project was certainly a noble vision when it was established in March of 2007, and at the start it was accorded a modest budget of 300 million a year to perform its duties. Because of subsequent events that do not need to be spelled out here, at the time of writing the annual budget for the project is expected to be 53 million, one-sixth of the original level. Already the managers of the project have realized that the 2012 target for completion cannot be met (Sigurðardóttir, 2010).[17] The project is seen as an easy place to cut because the cut will not lead to direct loss of jobs, but the fact that the project is meant to decrease public spending was not taken into account. The task of the government is to cut short term spending, not look to long-term matters. Despite the huge cut in budget, there is still some advance in creating the island.is site even if not along exactly the same lines as the original e-nation project, including vigorous security testing so that the site is safe to hold private information. Security matters are considered very important for the project, with independent companies handling security consulting and testing. Although Island.is has not itself come under cyber-attack the matter is handled pro-actively with regular testing of the site along with many other governmental sites (Sigurðardóttir, 2010).

[17] Interview with Guðbjörg Sigurðardóttir, Office Manager at the Department of Administrative Development with the Prime Ministers Office. Conducted at the 26th of March, 2010.

4.1.2.2 Iceland as a cyber-community: general challenges

Up to now, in spite of the high level of Internet use including almost universal use of online banking, the general level of security awareness among the Icelandic public seems to be minimal. This may be based on the fact that for a long time there was much trust in Icelandic society, and people did not worry about security aspects. In recent years this awareness has been rising, but is still very far from the appropriate level. This also means that the restraint level from the public towards their representatives is not very high, which would be considered a bad thing. Already there are projects in place working through the schools, where children are learning about the dangers of the Internet and connected elements, which then should lead to further awareness within their families (Sigurðardóttir, 2010). It can be wondered if this great threat should not be fought at more levels at the same time.

Partly because of low public awareness the vulnerability of Iceland's cyber-systems has long been kept a secret, or at least not advertised. It does however not take any expert knowledge to notice that there are several aspects of the country's infrastructure that are vulnerable. The ISPs are few and many of them are interconnected, which can make them more vulnerable in case of attacks or accidents. It was mentioned that in the case of Kyrgyzstan there were 4 ISP's. In Iceland there are effectively 3 ISP's, and 3 DNS[18] servers. While the security of these servers is in the hands of the ISP's, it can be said that much of the countries security is in the hands of private actors (Skúlason & Finnbogason, 2010). The sea-cables leading from the country are few, which makes the country's connectivity to the mainland more vulnerable (Stefánsson, (PTA) Conducted via email, 2010a). As in all fields of infrastructure, the first step must be to 'map' such vulnerabilities before desperately needed work for protection and resilience can finally begin. This has been done to some extent by the National Commissioner for the Iceland Police and the Civil Protection Department. There are contingency plans in place for many of the possible disasters and incidents that could occur in Iceland, but there are still some lacking features, for instance against botnets. While there are plans in place, there is still the unused option of

[18] DNS servers provide the name for any given website instead of a IP address. Disabling a DNS server would make these names unusable and most sites would become unaccessable. (Wikipedia, 2010)

actually preventing many if these incidents, which has not been done to a full extent (Pétursson, 2010). Awareness about these threats is present among the higher-level executives of Icelandic companies and among infrastructure operators, but the measures needed to respond to these threats are still unclear. Icelandic politicians are not thought to be quite aware yet of the threat, but it is seen as only a matter of time before that will change. There is some international pressure on the Icelandic elite to respond to the threat, which must finally start getting through (Stefánsson, (PTA) Conducted via email, 2009). As of now it could perhaps be easier and more time-efficient to raise awareness through the public, which would then reach the politicians through public pressure.

To tackle the actual problems of cyber-security, the number of qualified experts Iceland is said to be around 10 people. Although this is hardly a large number, it is very close to the number in Estonia in 2007, and the closeness of that group was an important aspect in defending against the cyber-attacks. The only difference is perhaps that the Estonian network was a close network of friends who cooperated on security issues. In Iceland there is hardly any cooperation between individual experts in the field of cyber-security, or any field of security for that matter. In the event of a large scale cyber-attack on the country it can be assumed that the defence would be conducted in a similar way with everyone working in their own respective corner, defending their own piece of the countries' infrastructure or private sphere. The defences for the actual state would probably be minimal, although it is of course clear that the companies and agencies cannot function without the state. Such an approach to defence is like saving a room, while the house burns down. It should also be kept in mind that any possible cyber-attacks against the country do not have to originate outside the country, and it is sometimes claimed that around 70 percent of attacks against a nation's web-sites originate inside the respective country (Símonarsson, 2010). It is then not enough to close all access from the outside world, the interior needs to be secured as well.

To mention one last general problem: data security was traditionally not an issue in Iceland, with valuable personal information available for all to see. The National Registry can be used as an example, where for a long time the social security number of every Icelandic person was available online to be accessed

without much difficulty. It took examples of that information being used for commercial gains for the access to be limited (Morgunblaðið, 2004).[19] Even if the practical repercussions were not serious, in most countries such openness would be considered a clear case of a violation of privacy. As Icelandic companies have become more competitive and internationally linked, however, the security requirements have risen substantially, to the benefit of the Icelandic public. It should be noted that the provision of online security has become a big business like any other, where companies work to maximise demand and coverage with the goal of making money. There have been large advances in specific areas of security, for instance the ID code required by the banks, and that technology is still evolving in Iceland. The real problem is that the progress made so far has not been through a wider cooperation between the state and/or private players involved, so that no comprehensive information is available about how things are going or on what protections have been achieved and what is still needed for the Icelandic case.

4.1.2.3 Security of commercial services

Credit card usage is high in Iceland as in most other developed countries, but Icelandic measures for the security of these transactions are lagging behind the international average. International standards for maximum security are laid down by the large credit card companies, but the discretion on how to apply these standards is placed on the companies themselves, at least in Iceland. The fact that companies that are fully verified and those that only claim to be verified are able to operate on the same footing could be counted against the state, but the blame can be hard to pinpoint. According to Jóhannes Ingi Kolbeinsson, Manager of Kortaþjónustan, lack of security awareness amongst the people leads to less pressure on companies to perform according to standards (Kolbeinsson, 2010). This view is supported by many other experts. It could then be said there are two options when it comes to raising the awareness of the people: communicating directly to the people or through the state. As was seen in the previous section the raising of awareness can be difficult, as some companies have turned to scare

[19] Grænfriðungar senda bréf til íslensks almennings. [Greenpeace sends letters to Icelandic public] Morgunblaðið. 05.05.2004. URL: http://www.mbl.is/mm/frettir/innlent/2004/05/05/graenfridungar_senda_bref_til_islensks_almennings/

tactics to try to get people to think about (and purchase) security protection. This cannot be the best solution, and a better way would perhaps be for the state to more actively enforce security standards on companies in various trades so that the people do not have to pressure the companies. The Icelandic government has used its institutional powers to raise certain standards, for instance regarding web-site security, so this would not have to be a stretch (Kolbeinsson, 2010).

Data centres are a rising industry in Iceland as well in other parts of the world. Iceland is considered a good place for a data centre because of the clean energy available in the country as well as the relative stability of the country. One of these data centres is being set up by Verne Global at the belly of NATO's Keflavík site. When Verne was first looking at Iceland there was a limited number of sea-cables running between Iceland and either Europe or North-America, and Verne in fact lobbied for the two latest cables, Danice and GreenlandConnect (Cantrell, 2010). The establishment of these two cables has made the data centre circumstances in Iceland significantly better, and according to Verne the future is good. While it is assumed that the cables equipment can fail it is possible to make contingency plans, and now that the new cables have been established the chance of downtime has been decreased. Verne Global's main customers are large industry leaders. Their traffic will be distributed over the various cables so that the domestic traffic should not be affected (Cantrell, 2010). It is especially interesting to note that Verne was able to lobby the Icelandic government into adding two more cables, although of course it is hoped that the cables would eventually have been connected, and Verne was also involved in many of the decisions made to make the connections possible.

4.1.3 Critical Infrastructure in the News

A few incidents have made the news in the last years that seem to point to Icelandic vulnerabilities, especially in infrastructure. They underline that since accidents occur at random, there could be more vulnerabilities that have simply not come to light yet.

An electrical malfunction in Vodafone's London system meant that Icelandic people in Frankfurt and other parts of Germany could not be contacted on their mobile phones. The malfunction did not last for more than one day but

still indicates that there are some deficiencies in the connection from Iceland to other parts of the world (RÚV, 2010).[20]

At the end of February of 2010 the FARICE sea-cable that runs from Scotland through the Faeroe Islands to Iceland stopped working altogether. The cable carries much of the Internet traffic from Iceland to mainland Europe, and while there are some who were moved to alternative cables and would then not feel much disturbance because of the malfunction, there are still some who felt the disturbance. The malfunction occurred in Britain, but caused a decreased Internet traffic in Iceland (RÚV, 2010b).[21] It can then be assumed that any institution or agency that was only connected through the FARICE cable would be unconnected until some backup connections were made.

The rural areas of Iceland are more vulnerable than others when it comes to infrastructural connections. Electricity supplies in the Northern Westfjords are routinely going offline, for instance because of icing and bad weather, with some towns and houses being without electricity for several hours (Bæjarins Besta, 2009).[22] While this might not seem to be serious, it should be noted that this is quite frequent, and Iceland does consider itself a developed nation. There is also a reasonable likelihood of electric cuts being combined with other events in which case the situation could become very serious. Most of the country's infrastructure is of course heavily dependent on electricity, and backup generators only have a limited capacity. In the case of a long term electrical outage, serious problems in both national and personal security could develop.

In March of 2010 an act of sabotage was attempted in Iceland. The act was badly planned and badly executed. Three small 'bombs' were attached to important communications masts in Reykjavík, which carried antennae belonging to the biggest communications companies in Iceland. Had the attack been successful it could have affected cellular and micro-wave connections throughout the country, but the full extent of damage can perhaps not be fully described. The

20 Rafmagnsbilun truflaði símasamband. [Electrical malfunction interrupts telephone connections] 31.01.2010 Ríkisútvarpið URL: http://www.ruv.is/heim/frettir/frett/store64/item323085

[21] Ekkert samband um Farice [No connections through Farice] 28.02.2010. Ríkisútvarpið URL: http://www.ruv.is/frett/ekkert-samband-um-farice

[22]Rafmagnstrflunir á Vestfjörðum.[Electrical distrubances in West Fjords] 03.12.2009. Bæjarins Besta URL: http://www.bb.is/?PageID=26&NewsID=141301

area where the masts were situated were not very well guarded, with no personnel at the location, and it was neighbouring people seeing the fire caused by the bombs who contacted the authorities. The area was not guarded by surveillance cameras, so law enforcement officials have been forced to watch surveillance cameras from gas stations in the neighborhood to try to find the guilty parties. The only possible good that could come from the event is that the Minister of Justice has announced that the matter will be examined further (Morgunblaðið, 2010c).[23] It is a matter of greater concern that it took an actual attack, although a poor one, to force the government to look seriously at the risks. This could be taken as an indication that the Icelandic government is more prone to reactive functioning than to being proactive on security.

In March of 2010 a volcanic eruption began in Eyjafjallajökull, on the southern coast of Iceland. Immediately contingency-plans went into effect, shutting off airplane traffic and evacuating all the people who might possibly be in danger because of lava or ashes. Roughly six hours after the supposed start of the eruption, over 500 people had been evacuated, with roadblocks so that no one might get into the threatened area without the police knowing about it (BBC News, 2010).[24] All possible angles to the eruption have been estimated, with the eruption possibly waking another dormant volcano and thus making the situation much worse. There is also the possibility of floods caused by the lava, which could threaten human lives and ruin roads. This experience underlines that natural disasters such as volcanic eruptions have been well planned for, while other possible disasters, notably of the man-made variety, have not been planned for at all. The volcano in Eyjafjallajökull last erupted in 1821, while most countries are threatened by cyber-weapons many times every day. It can be wondered which disasters are really the most likely to catch Iceland off guard.

Although each of these incidents was in itself not extremely serious, it could be assumed that if two or more were to happen at the same time the results could be disastrous. The fibre-optic cable that circles the country has been cut on numerous occasions by accident, and while these incidents have for the most part

[23] Communications will be better guarded. [Fjarskipti verði betur varin] 19.03.2010 Morgunblaðið URL: http://www.mbl.is/mm/frettir/forsida/2010/03/19/fjarskipti_verdi_betur_varin/
[24] Volcano erupts near Eyjafjallajoekull in South Iceland. 21.03.2010 URL: http://news.bbc.co.uk/2/hi/europe/8578576.stm

only caused minimal damage, if they coincided with other elements of emergency the country could very well become paralyzed to some extent. It can also be mentioned that if the circled fibre-optic cable would be cut on two sides, this could limit the connectivity of Reykjavík to a very large extent, with unthinkable consequences. It can then also be assumed that in the case of a well planned attack, any attacker would know where to attack, and in the case of an attack on two simultaneous places at once, the repercussions could be extreme.

4.2 Solutions for Icelandic cyber-security and infrastructure

What changes are then needed in Icelandic society so that the country will not become an easy victim for some fourteen-year-old novice hacker or the more sophisticated cyber-criminal who sees this small country as a quick way to make large sums of money? The starting point for looking realistically at any such security issue in Iceland is to recognize that the Icelandic community has long been a peculiar one. Due to the arrangement with the US, traditional defence has not been a real issue in the country for a long time, with someone else handling the matter for the state. Now that Iceland needs to look to its own security, that old mentality is still present. The privatization of Icelandic infrastructure also seems to have created special circumstances, with what resembles a 'clique' mentality still all too often persisting within the state. While all should be working on the common cause of keeping the country safe and running, everyone seems to stay very much in his/her own corner, working on their own concerns.[25] Of course it is to the benefit of all Icelandic companies and institutions that Icelandic infrastructure and society should be safe, and everyone who needs to be involved should be involved. Yet cooperation when it comes to security is also non-existent, not only within the private sector but also to a large extent within the public sector (Böðvarsson, 2010). Cooperation between ministries and institutions under them is also minimal.

The main exception to this would be the National Commissioner for the Icelandic Police. The Commissioner has taken steps to coordinate efforts within the department itself, and there is also cooperation within the department and to

[25] This can for instance be seen in Landsvirkjun and Landsnet. While being *de facto* the same company, there is still some friction about certain directions after the division of the company. This is referenced in section 3.1 of the 2009 Kerfisáætlun accessible at http://www.landsnet.is/Uploads/document/skýrslur/Kerfisáætlun_2009_lores.pdf

the Ministry of Justice. This seems to be to a greater extent than in most other Icelandic institutions. The Commissioner is also participating in international cooperation to a large extent, for instance heading NATO civil missions and working very closely with the EU, for instance in the Schengen cooperation. There is also the Coordination Centre for the Icelandic Civil Protection Department, which is ahead of many countries in terms of coordination.[26] At the centre every possible actor that should have a place at the table gets at table, so that sharing of information in times of crisis can be as quick as possible (Pétursson, 2010). It should be stated that there are still several factors lacking in the work of the Commissioner, but in times of recessions many ministries and institutions are starved of funding in many regards. These budget costs have been very serious for many security measures, and many pro-active police activities have been cut. That places the bulk of responsibility on re-active 'after-the-fact' police work, which in most cases results in higher costs for the state. This is a clear example of the short-term thinking often presented in Icelandic society. The National Police Commissioner is also one of the few institutions that seem to have examined the published Threat Assessment to see what should be addressed by the Commissioner. The question of whether cyber-threats should be covered by the department has also been discussed, but in light of the fact that these matters are generally covered by military departments, the Police Commissioner has not assumed the responsibility (Pétursson, 2010). In times of recession departments might be unwilling to assume more tasks to place under an already strained budget.

The most obvious and effective way to deal with as large a matter as cyber-security would require the cooperation of the entire Icelandic society, with a centralized agency involving both the private and public sectors as the fittest vehicle to preside over that cooperation. As will be presented in the next chapter there are several opportunities for Iceland to seek help and cooperation on the international scene, but there are also possibilities within the country. The Icelandic Defence Agency receives information about security threats through NATO, and this information could in some respects be used to protect the country and to prepare advice about how the security of the infrastructure should be

[26] The Centre has been used as a model for other countries, for instance Norway. (Pétursson, 2010)

handled. The personnel of the Agency have had experience and advice from NATO for several years and could help to devise security measures for more than just the Agency's own use (Símonarsson, 2010). While the Agency itself is supposed to be disbanded, the employees and available hardware is still present and can be used for this very important task.

So far, the main official study on a possible central solution in Iceland has been the one carried out on establishing an Icelandic CSIRT team and this is discussed in the next sub-section.

4.2.1 A possible national CSIRT team in Iceland

The Ministry of Transport, Communications and Local Government[27] published a report in August of 2008[28] regarding the possible establishment of a CSIRT team in Iceland, and asked several individuals connected with Icelandic defence and infrastructure to review the report's recommendations (The Ministry of Transport, Communications and Local Government, 2008). [29]These individuals came from telecommunications companies, universities, the banking network and the Iceland Defence Agency, to name a few. Their comments have been published without attribution, which is thought to result in better and more truthful answers (The Ministry of Transport, Communications and Local Government, 2009).

The report explains the functioning of a CSIRT/CERT[30] team and looks at the Icelandic situation in detail. There are a few different types of CSIRT teams available, the most important one being a national CSIRT team. That team handles the nation's defences, coordinates all national efforts, and provides a venue for cooperation and a framework to evaluate the relevant dangers. The countries most often compared to Iceland have a national-CSIRT already:[31] for instance the Nordic countries all have such teams, and the European Union is said to value CSIRT teams as a cornerstone of the protection of important communications and information infrastructure for the coming years (The

[27] Icelandic: Samgöngu- og Sveitastjórnarráðuneytið
[28] Report is available at URL: www.samgonguraduneyti.is/media/frettir/Kynningarskyrsla_um_forystu_CSIRT_a_Islandi.FINAL.pdf
[29] The review document is available at http://www.samgonguraduneyti.is/malaflokkar/fjarskogpost/frettir/nr/1899 (Icelandic)
[30] CSIRT is thought to be more appropriate name and will be used in this chapter.
[31] Also known as Governmental-CSIRT team

Ministry of Transport, Communications and Local Government, 2008, p. 6). Other possible CSIRT teams are for instance University CSIRT teams and teams established for important closed networks. This is for instance the case in the Icelandic Defence Agency. There is no national CSIRT team active in Iceland at present, as the communications companies have for the most part handled any immediate dangers individually or perhaps in smaller groups without any central coordinating power (p. 6).

A national CSIRT team is made up of representatives from interested parties, for instance security teams for communications-, electricity- and financial companies, the health industry, law enforcement, universities and research institutes, and these are bound by a written agreement. The national CSIRT team is concerned with the needs of such actors but not necessarily with the security of the individual. The team is also connected with foreign CSIRT teams and other actors that might have requests or advice regarding Iceland's computer security. The team also participates in international cooperation regarding possible solutions to security issues (p. 7). It analyses and collects information about possible weaknesses in the nation's infrastructure and provides possible solutions to these weaknesses. Information should be delivered quickly through the team to the relevant parties so that remedies can be applied. Contingency plans should be in place and should be easily executed. A regular and close connection must exist between the team and the media, as the CSIRT team must be able to answer any request that might come up regarding possible threats. The tasks of the national CSIRT team are not necessarily limited to the protection of the communications and information systems of a nation. The team could also handle the protection of more limited communications systems or cellular networks, to name a few examples.

As with any other actor in the security industry, trust is a very important factor. The trust between the CSIRT team and the parties involved can for instance be damaged if the team suffers from a lack of funding so that its efficiency is called in doubt. That loss of trust can be hard to remedy. However, the source of funding could be disputed as some might argue that protection of the private industry should not be the responsibility of the state. On the other hand relying on private funding for cyber-defences could raise some suspicion of

favouritism when it comes to prioritizing possible threats. The last point would be that if the private sector handles at least part of the funding that would guarantee their participation in the project (p. 7). That is only one possible option, while the most convenient option will be discussed later in the section.

The initial Icelandic report on a CSIRT is of course based on the experiences of other countries, which have shown that it can take as much as two years for a CSIRT team to achieve the trust required to perform its tasks. It can take eight to nine months for the team to be operational after the employees have been hired, and a minimal staff requirement would be 4-5 employees to begin with (p. 8). The report goes on to offer three possible solutions for an Icelandic national-CSIRT team. The first solution requires 5 employees, who would handle the possible threats posed to the Internet, general telecommunications system and other systems. The funds required for this option are around 49 million Icelandic Kronur, with an annual 42 million in salaries and other costs. It should be noted that the report was made in August of 2008, so the figures mentioned could need updating. The other options mentioned in the report are more limited, with initial costs ranging from 41 million to 30 million, and annual costs of 37 million and 26 million respectively. The lower cost would be achieved with fewer employees, less defences and more dependence on foreign help in the protection of Icelandic systems. It is noted that in the case of a global threat it could not of course be guaranteed that foreign teams would assist Iceland when faced with threats in their own countries (p. 8). On the number of employees required for this type of team, most would agree that several more are normally needed, and the typical number has been around 15, which would be on par with the other Nordic states (Stefánsson, (PTA) Conducted via email, 2010d).

The report comes to the conclusion that cyber-threats pose a serious risk to Icelandic infrastructure. When asked if they agreed with that conclusion and whether the government should respond to the threat, the individual experts consulted mostly agreed that a serious threat is present, and that certainly the Icelandic government should act in the nation's defence. It was noted at the same time that Iceland is not in any more danger than most other countries, and there is also the suggestion that operators of larger computer systems should not have an

active part in the national CSIRT team but would rather be recipients of information about present dangers.

When asked about the three proposed options regarding the establishment of a national CSIRT team, the experts' answers are more diverse. While at least two prefer the first and largest option, there are also some who mention the other smaller options (The Ministry of Transport, Communications and Local Government, 2009). There is also a possibility of starting with the smallest model and then evolving into the larger options if needed. Another approach would be to perform a full-scale national threat assessment that could be used to determine which option should be chosen. One individual stated that the best option should be to try to reach an agreement with a foreign CSIRT team, since it can be assumed that a larger state would be better able to fight the threats and that this would be a way to save resources. Another possibility mentioned is that relevant parties in Iceland should come together to create a CSIRT-type team, but without the direct coordination of the state. The government could perhaps fund one employee and this group could meet on a regular basis, looking into the threats facing the country. This solution would become operational more quickly than the national CSIRT options in the original report.

The placement of such a national CSIRT team can be questioned, as the different ministries or governmental organizations have varying qualifications to handle its operations. Most of those consulted agreed that the team should be situated within the government, but some differed on the specific place. Three main reasons were given for a governmental solution. The first is that the state is the main beneficiary of the team, and therefore should be closest to the team itself. The second is that the CSIRT team would at times have to appear as a representative of Iceland, and the trust required for that can only be gotten by situating the team within the government. The third is that in the case of security, the profit motive alone may be a risky guide and – as discussed earlier in this thesis – that is one of the basic rationales for putting security under the control of the state. The place most often mentioned for situating the team within the government is the Icelandic Post and Telecommunications Administration (PTA). The PTA falls under the Ministry of Transport, and the CSIRT team could also fall under that ministry, as a sort of 'sister-department' of the PTA, or even be a

joint effort by the Ministry of Transport and the Ministry of Justice. One final suggestion is that the team could be placed under the Icelandic Defence Agency, for which a case could certainly be made, but – as noted - since the publication of the report the government has decided to redistribute the functions of the Defence Agency between other official bodies. A suitable place for a national CSIRT team could present itself in the aftermath of that distribution.

The last question is a matter of funding for the possible CSIRT team. Most agree that the state should handle the greatest part of the cost for the team. Certain symmetry can be seen with the police force, as both entities work on security matters. Neither entity is selling its services to the people they handle, so that the best solution is state funding. It is also mentioned that many corporate leaders see security as mainly a cost, and could then be tempted to keep that cost as low as possible. However, even if the government handles the funding to begin with, that does not need to be a permanent solution, and could be changed as the team becomes better rooted in the Icelandic security environment.

Other comments made by the experts consulted included a warning that there are no guarantees that Icelandic companies will cooperate with the national CSIRT team if it is not in their immediate interest to do so. For instance in the case of a virus-infected computer that is connected through an Icelandic Internet Service Provider, that ISP could be hesitant to limit the connectivity of that computer because of monetary concerns. This problem can best be handled with very close cooperation between private and public actors. Other comments are for instance that there are plenty of foreign companies and teams fighting cyber-threats, and it cannot be a good idea to take the few individuals that are available in Iceland and make them work in competition with these foreign individuals. Since these foreign teams are sending threat assessments and warnings around the world, according to this commenter there is really no need for an Icelandic team.

Overall, it is clear that some of the ideas in the initial assessment have more endorsement among the consulted representatives than others: and that a larger national CSIRT team with a minimum of 5 employees, established within or alongside The Post and Telecommunications Administration, may be considered the most favoured solution.

4.3 Conclusions

While cyber-threats might not be the biggest threats that Iceland faces, they are one of the most relevant and potentially the most complex in their impact (Símonarsson, 2010). There is much need for enhancement of general and specific expertise within Icelandic society, for instance within the Icelandic Police Force. Special computer departments need to have the training and hardware that is required to be able to successfully investigate computer offences. And although no judgement will be made here on the capability of the police force to investigate these types of crime, more training and hardware can hardly be considered a bad thing. International cooperation along with partnerships within the Icelandic community would increase the rate of prosecutions and make the whole process run more smoothly.

To meet Iceland's needs overall it would seem that the best solution would be a centralized authority that could handle all aspects of cyber-security and critical infrastructure. This centralized authority could handle the distribution of public information, act as an information hub between private companies so that no loop-holes are left open in the country's defences, and help to pull Iceland's limited community of experts closer together. The smallness of the country offers opportunities, not only hindrances, in this context and these should be exploited. This authority could in fact be a CSIRT team of sorts that could be adapted in design to reflect the smallness of the country. CSIRT teams have for instance been known to handle exercises to determine how vulnerable a country's infrastructure might be, and that would probably also be the responsibility of an Icelandic CSIRT team (Stefánsson, (PTA) Conducted via email, 2010c). The CSIRT team could also provide the crisis response team that the Threat Assessment calls for, and would act as a liaison point between Icelandic and international cyber-security efforts as covered in chapter 5. As was stated in chapter two, and confirmed by experts, the statements of private companies about present dangers are always taken with some scepticism which a centralized entity could avoid (Skúlason & Finnbogason, 2010). In some cases these private companies can be better informed about imminent dangers and what is going on in their respective societies, so the communications between private companies and this possible CSIRT team would need to be very good if a monetary connection is not present.

There is also a clear need to educate the public, and to raise awareness of the issue. There are Icelandic websites that are designed to inform the people of the dangers, but these websites have not been visited often (Stefánsson, (PTA) Lecture on Security and Information, held by SKÝ, 2010). As always in such cases, while the issue of what could be called cyber-hygiene of a site is kept hidden there will always be a sort of shame connected with possible infections, but with openness and clear advice the shame will be removed. There are certain efforts underway in Iceland, but there is still a long way to go in this regard. Although the education through the school system will most likely deliver results, this can be called a long-term plan, while more short-term actions are needed. Perhaps advertisements or news reports could be carried in the mass media about what can happen on the Internet and the dangers that could easily affect Iceland and Icelandic people in this inter-connected world: but as was stated before, scare-tactics should be avoided. The most important factor here is trust, so the agency that offers warnings and advice regarding security issues needs to have the trust of its constituency – a point also made at the conceptual level in the securitization section of chapter 2.

In the last resort, if a state is seen as unable to handle its own defences maybe it should become a responsibility of other neighbouring countries or other members of the international system to intervene. This is especially the case when the relevant threat is a global threat that can spread from an infected country to other places, and this could equally well be the case whether the country is Burkina Faso or Iceland. Even if Iceland might not be pleased to be grouped with a developing African state, any country that falls down on its responsibilities must face the possibility of being placed on a par with similar countries. As will be pointed out in the coming chapter there are plenty of international opportunities for states that are reluctant to invest too much money in their own cyber-security, so no country needs to be left behind in this field. Iceland has for a long time been a ‘taker’ when it comes to international cooperation, for instance through the defence agreement with NATO and the US, and in many other regards (Símonarsson, 2010). It is perhaps time for Iceland to start being more of a ‘giver’ in international cooperation. While the smallness of the country has often been

named as an excuse for a lack of cooperation, any large task begins with a small step.

In fact, even if Iceland is small by anyone's standards and is affected by this in more fields than many others, there are effectively three basic strategies that can be adopted by any such state when facing a problem such as cyber-threats. The state can use its influence and authority to create a small niche for itself, so that the expertise of the country would also be valuable for other states thus helping to share the costs. The second strategy would be to seek protection from a larger national power, and the third would be to enter cooperation with one or more international institutions/agencies that possess power and influence, thus gaining strength in numbers in the collective fight (Bailes, 2010). It should also be noted that the first and third strategy can be applied together, and the third option would perhaps even be stronger if the first option was chosen and acted on beforehand. And while smallness is often described as a hindrance, that does not need to apply to Iceland in the present international situation, where it could offer its ideas and expertise as an impartial intermediary instead of being seen as a lackey for some larger power. This would be beneficial for all involved, in all or at least many of the available institutional frameworks to be described in the following chapter (Bailes, 2010).

At the same time, one of the worst recessions of history is gripping Iceland in 2010, and a massive cut in public spending is required. The clear message of this thesis is that spending on vital aspects of security – including those that underpin the economy itself - should not be cut, but also that a long-term view should be attempted, as there is always a light at the end of the tunnel. The Threat Assessment that was made for the country in 2009 already needs updating: but a good start would be to work on those recommendations in it that have yet to be implemented, and which could improve security and contingency planning immensely.

5 Why a transnational approach? Who can help us?

As the threat posed to the country is international in nature and respects no boundaries, it seems natural that help should be sought from the largest possible combination of partners: individual countries and international institutions, as well as non-state actors. In this section the major relevant international bodies are examined and their efforts to find an answer to the cyber-threat are looked at as possible sources of aid in Iceland's fight. Of course, Iceland can hardly expect to be purely a recipient of help in this context and would most likely have to commit some resources as well.

Here we look at the idea of reciprocal aid first in the context of the 2009 Stoltenberg Report and its proposals for using Nordic cooperation – a fitting arena for Iceland, which takes part as an equal member - against cyber-threats. As will be explained in section 5.1, Iceland has already begun cooperation with other Nordic states in this domain. However, Iceland's participation in international efforts does not need to end with Nordic cooperation, and Iceland could well become an active member in the fight against cyber-threats in some or all of the other settings covered later in the chapter.

5.1 The Stoltenberg Report

The so-called Stoltenberg Report was delivered in February 2009 by the former foreign minister of Norway, Thorvald Stoltenberg, at the request of the foreign ministers of all the Nordic countries. The purpose of the report is to enrich the cooperation between the Nordic states in the fields of foreign affairs and defence (Stoltenberg, 2009, pp. 25-26). Although the Nordic states may differ when it comes to membership in either the European Union or NATO, both these institutions encourage regional approaches to modern security challenges, especially between states that are members of different institutions. Stoltenberg's

thirteen recommendations all cover cases where cooperation between two states is encouraged as a starting point, with more states joining at their convenience.

The item most relevant to this thesis is the seventh proposal regarding cooperation in defences against cyber-threats. There Stoltenberg recommends the creation of a Nordic knowledge network that can be used in defence against cyber-attacks launched against the Nordic states. The main task of the network would be to exchange information and coordinate between the participants so that no nation is seen as being left behind. As time advances the network can evolve so that warning signs are coordinated and shared between the nations (Stoltenberg, 2009, pp. 25-26). The most critical sectors for cyber-defence according to Stoltenberg are land defences, aviation, trains, energy, telecommunications and financial matters. He notes that the methods or the culprits of a cyber-attack are effectively unknown, and are also evolving to certain degree. The attackers could be foreign states, terrorist organizations, criminal organizations and private individuals (Stoltenberg, 2009, p. 25). Stoltenberg goes on to argue that defences against cyber-attacks should be a part of the modern defences of every state. While the Nordic states should each have an institution that carries the responsibility and prevents operations launched against critical infrastructure, they also have different experiences and capabilities when faced with cyber-threats, and systematic Nordic cooperation in this field is needed (Stoltenberg, 2009, pp. 25-26).

This team that Stoltenberg recommends to investigate this issue has already been established in the beginning of 2010, with Iceland as participant and host. A meeting was held in February 2010 where individuals representing the appropriate ‘Point of Contact’ in each of the Nordic countries came together in Reykjavík, Iceland. The Post and Telecommunications Administration in Iceland is charged with looking into the establishment of a national CSIRT team, and thus represented Iceland at these meetings. This group will work, as per the Stoltenberg report, on establishing a communications- and information sharing network for the Nordic countries – the form and participants of which are still to be determined (Stefánsson, (PTA) Conducted via email, 2010b).

There is also a need for a secure method of communication between the Nordic states, the lack of which may prevent quick sharing of important information. As was seen in the cases of Estonia and Georgia the nature of cyber-attacks is that they are very quick, so time is very important in cyber-defence. In order for the Nordic states to successfully defend against cyber-attacks in a coordinated and efficient manner the countries must first have an evolved and secure communications system. Their cooperation can also involve technical solutions, the sharing of estimates of cyber-threats, analysis of methods of attacks, and information about critical sectors, as well as coordination over special defence measures. Cyber-matters are special in the sense that defence measures are also de facto attack measures, and so the matter needs to be examined extensively before any decisions are made (Stoltenberg, 2009, pp. 25-26).

There is already some international cooperation on cyber-security in the wider Northern region, for instance the 'Cooperative Cyber Defence Centre of Excellence' established on behalf of NATO in Estonia, which will be examined further later in this chapter. Nordic cooperation in the field of cyber-security will thus not only increase the security and cooperation between the Nordic states, but also enhances the contribution that the Nordic states make to existing international cooperation arrangements to this threat.

A certain hierarchy or 'subsidiarity' principle' can be applied to the options for cooperation on fighting cyber-threats. Stoltenberg recommends cooperation first between neighbouring states and then on a regional basis, which in turn can be used to supplement the cooperation of larger groups. One of the benefits of regional organizations is that states can coordinate on matters before they go into the larger international bodies to present their cases. Nordic cyber-cooperation would follow the same guidelines. In the event that Iceland was to enter the European Union, the Nordic countries would certainly make a strong bloc that could have a impact within the Union. The nature of cyber-threats, as has been stated on numerous occasions in this thesis, is to be pre-eminently a cross-border threat, and most would say that this kind of threat could not fully be fought on a traditional nation-to-nation basis. Stoltenberg also mentions that cooperation between the Nordic states could limit the resources wasted on double efforts (Stoltenberg, 2009, p. 28). This must certainly have a huge significance in an

atmosphere of limited resources. A Nordic bloc focussing inter alia on cyber-matters could certainly make an impact and help move international agreements and cooperation to a new level.

This emphasis on using cooperation to avoid duplication, and on feeding results from more specialized groups into larger institutions, is important for the whole discussion in this chapter. On the one hand more effort does not mean better if it re-invents something that another state or institution is already doing better elsewhere. On the other hand, solutions cannot really be complete until they have advanced to cover all possibly relevant actors. Among other things, there is not only a responsibility but an argument of self-interest for the more developed states to protect the less developed states. When a computer in a less developed country is not protected, that computer can be dangerous for all other computers and even for states, including in the developed world. If for instance a computer in Burkina-Faso is used to deliver spam to people in Iceland, that risk could be avoided if the cyber-security industry in Burkina-Faso were sponsored by the developed states, or even if the people of Burkina-Faso were educated about the benefits of anti-virus software. It is clear that cyber-systems make the world even smaller and inter-connected than most other threats the world of today faces. It can also be seen throughout history that common threats tend to unite differing actors, no matter the level of disagreement. Global warming has united many and varied countries in the fight against the threat, and so could cyber-threats unite states that otherwise would not come together. This will be looked at further later in the chapter.

5.2 The United Nations

The United Nations (UN), as the biggest international body in the world, has not surprisingly passed resolutions on cyber-security or relevant fields. Although the actual effectiveness of the extant resolutions can be disputed, they are no less important as a raiser of awareness. The most directly relevant example, resolution 57/239, was adopted in 2003 by the General Assembly of the UN. It recognises the growing dependence states have on information technology, and that this dependence is common through all stages from the individual through governments to international groups (UN General Assembly, 2003). It also states that cyber-security is not an issue just for states or law-enforcement officials to

handle, but should be tackled throughout society by intensive planning and management: indeed the responsibility for security lies with every user of information technology. International cooperation is best fitted as a means to combat cyber-threats, aiming for example at increased learning, improved public services and better and more reliable information technologies for every inhabitant of the world, not leaving out the people of developing nations. With the increased access to information technology, the dangers become even more present and sharing information with the newer or less prepared users becomes more vital.

As the whole world becomes connected to the Internet, the UN asks that all participants keep certain elements in mind. These elements are awareness of the security needed to sustain a information system and what can be done to enhance that security; responsibility for people's own actions and systems on the Internet; the need for quick responses to any threats that might occur and for the sharing of information about possible threats and vulnerabilities, also through cross-border cooperation; and an awareness of ethics in the sense that in the peculiar nature of the Internet, with every user connected to all others, inappropriate action and inaction could harm others even against the user's will. The resolution further notes the importance of democracy in the freedom to exchange information and ideas, of the freedom of expression, and the protection of personal information, along with openness and transparency. Risk assessments should be performed by all actors to determine threats and vulnerabilities that can be caused by internal or external factors, and the design and implementation of information system should incorporate security aspects to a high degree. Security management should be based on a risk assessment which is dynamic and comprehensive, and the notions of security should be re-evaluated regularly, with modifications made to address new threats and vulnerabilities addressed as quickly as possible (UN General Assembly, 2003).

The UN has also been active in the fight against terrorism, and as was seen in chapter two of this thesis, the dividing lines between cyber-crimes and terrorism can often be very thin. Although UNSC Resolution 1373 was adopted in the aftermath of the 9/11 attacks with the international support that followed, the resolution still constitutes a lasting accomplishment (UN Security Council, 2001).

It states that states should cooperate in their efforts to eradicate terrorist activity, for instance by implementing all viable conventions on the subject. All states should also make it as difficult as possible for terrorists to operate in their country, notably by freezing their funds and assets where possible and by cooperating fully with other states and international bodies.

The Economic and Social Council of the UN has also made its contribution to the fight with Resolution 2007/20 which revolves around international cooperation to fight economic fraud and identity related crimes (UN Economic and Social Council, 2007). While the Council recognizes that it may not be the most suitable agency to fight this threat, it draws attention to an existing convention designed to combat these types of offences on the Internet, namely the Convention on Cybercrime published by the Council of Europe[32] (which is examined in detail in section 5.6 below). ECOSOC encourages member states of the UN to sign and ratify the Convention as well as other international agreements made to combat this and other similar threats. Finally, the UN has also recognized the role that the Internet plays in terrorist activity. As was seen in section 4.1.2 terrorists use the Internet to a large extent, for instance in recruitment and to publish their message. There is a large-scale movement to address this threat, with the UN offering technical support in terms of legislation and the building of legal capacities.[33]

5.3 NATO

Cyber-attacks against NATO member states first gained serious official recognition within NATO at the Prague Summit in 2002. After the terrorist attacks of September 11th of 2001, NATO members had been made aware that there was a need for the organization to adapt to a whole range of new threats, even if the connection between terrorism terrorist threat itself and cyber-threats was not made as clearly by NATO at the time. Heads of State and Government agreed to strengthen NATO's capabilities to defend against cyber-attacks (NATO - Prague Summit, 2003, p. 74), limiting the decision however to the protection of NATO's own system and the capabilities to communicate within the organization,

[32] The Resolution is available at URL: http://www.un.org/en/ecosoc/docs/2007/resolution%202007-20.pdf

[33] This movement can for instance be seen in the Sixtieth session of the General Assembly at URL: http://www.un.org/unitingagainstterrorism/sg-terrorism-2may06.pdf

rather than to the systems of member states. The Prague Capabilities Commitment (PCC) adopted at the same Summit, which focussed on requirements for modern force deployments, also included the need to improve control and communications (NATO - Prague Summit, 2003, p. 11). In 2002 followed the establishment of a CERT team of sorts for the Alliance. The bureau is called NCIRC (NATO Computer Incident Response Capability) and was installed in SHAPE. It provided a forum for cooperation between the CERT teams of the member states where experts can share information and improve the knowledge that is already available. The NCIRC also stimulates the establishment of new national CERT teams inter alia through workshops that it holds on a regular basis (ENISA, n.d). At the Riga summit in 2006, the need for protection against cyber-attacks was again voiced in view of the possible disruption of NATO and national infrastructure assets (NATO - Riga Summit, 2006, p. 12).

In April of 2007, a NATO member state came under cyber-attack for the first time in history –i.e. the Estonian incident described in chapter 3 above - and for the first time NATO received a request for aid against a digital attack. What the Estonian case also made clear to the NATO representatives was that the organization was nowhere near ready for attacks on this scale, even though (as discussed earlier) the severity of the Estonian attack was not very high. In the following summit at Bucharest in 2008, cyber-attacks accordingly received much greater attention. The summit noted that a new NATO Policy on Cyber Defence had been adopted, and called on NATO's member nations to use their best efforts to protect critical infrastructure systems and make available assets that might be used to help other NATO members facing cyber-attack (NATO Bucharest Summit - Section 47, 2008). In further developments following the Bucharest Summit, a NATO Cyber Defence Management Authority (CDMA) was set up in Brussels to act as a centralized coordination bureau so that any member state can answer cyber-attacks with full force. The Authority is to have a real-time threat pin-pointing mechanism and to have the ability to share cyber-information as quickly as possible. Future predictions state that the CDMA will be a 'war-room' for cyber-attacks, where the cyber-efforts of the member states will be controlled through a 'coalition of the willing' (Hughes, 2009). When Estonia was under cyber-attack, it was hard to know exactly who to contact to ask for assistance, but

the CDMA should effectively become the unit to contact in such cases of emergency. The coordination the CDMA provides also ensures that duplication of effort is minimized in the fight against cyber-threats.

Another important development in the aftermath of the Bucharest Summit is the establishment of the Estonian Cooperative Cyber Defence Centre of Excellence (CCD-CoE). This is not an operational centre *per se*, but rather a new element of the International Military Organization referred to in the North Atlantic Treaty, as per article 14 of the Paris Protocol of 1952[34] (CCD-COE, 2008, p. 5). The Centre is not funded by NATO, but by a group of sponsoring states while Estonia as the host carries the administrative and infrastructural cost. Each sponsoring state is responsible for the salaries of its representatives at the centre and also a contribution to a shared operational budget (CCD-COE, 2008, p. 7). Although a certain connection might be drawn between the fact that the CoE is placed in Estonia and the cyber-attacks against the country, the truth is that Estonia had fought for the establishment of an Estonian Centre for several years. The sad fact is that it seems that it took a cyber-attack against the country for NATO finally to agree to establish the Centre. The Estonian Centre has evolved since 2008, and has for instance enriched its cooperation with the private sector through a declaration of understanding with the anti-virus company Symantec which commits the two parties to cooperate on research on the nature of online threats. When the nature of the threat is better understood, the threat can – just as in other fields of security - be better fought (CCD-COE, 2010).

At NATO's Strasbourg/Kehl Summit in 2009 the matter was again addressed, although there were no real significant changes. The protection of critical information infrastructure within the organization and the member states was declared to be of great importance, as the alliance and its members are putting more reliance on these systems, making them a tempting target for attackers. The Summit statement greeted the closer cooperation between NATO and its partners on protection against cyber-attacks and stressed the general need for international cooperation in this field (NATO - Strasbourg/Kehl Summit 2009 - Section 49).

[34] The Paris Protocol is available at URL:
http://www.nato.int/cps/en/natolive/official_texts_17300.htm

A still open question about NATO's cyber-role is how to relate cyber-attacks to Article 5 of the Charter which states that an attack on one member of NATO should be considered an attack on all members. There is of course no mention of cyber-attacks in the charter as the idea had not been invented at the time of writing, and to some the notion is still a bit far-fetched. As things stand and given the usual uncertainty over the source and motive of any such attack, several countries would not be willing to commit to applying Article 5 automatically to any cyber-attack claimed by another member. Nevertheless, the likelihood that the next great fight of the world will start with a cyber-attack is thought higher than it was only several years ago (Boessenkool, 2010). This can of course be seen in the case of Georgia, and it seems clear that the nature of warfare is actively changing.

Another rationale for continued and perhaps growing NATO involvement is the new emphasis the Alliance has placed on Civil Emergency Planning (CEP), as part of its effort to develop a new rationale after the Cold War (NATO CEP, 2006).[35] The aim of CEP cooperation is to collect and share information on national contingency plans, including for civil emergencies, so that national capabilities can be brought to bear and coordinated effectively without loss of time. Relevant events could include natural disasters such as earthquakes or floods, but also man-made disasters that could have a serious impact on the health, safety, security, economic welfare and the effective functioning of the state. While member states will handle emergencies within their own nation, many events can quickly spread beyond their limits given the interconnectivity of modern societies. NATO will then act as a forum for comparing and analyzing so that cross-border emergencies can be handled jointly if needed. NATO CEP procedures have for instance been invoked in the US after Hurricane Katrina, in Pakistan following the earthquake of 2005 and in the aftermath of the 9/11 attacks and the terrorist attacks in Europe in 2004 and 2005. NATO has also focused on enhancing national responses to possible attacks using chemical, biological, radiological or nuclear agents. In general NATO CEP encourages international cooperation, sharing of information such as threat assessments, and best practice including in the field of training and education to ensure that all nations understand the

[35] The report on NATO CEP is available at URL: http://www.nato.int/docu/cep/cep-e.pdf

importance of critical infrastructure for their society and to the international community (NATO CEP, 2006). Clearly, IT infrastructures are an important aspect of the assets that NATO seeks to protect through CEP, and the relevant NATO authorities work accordingly to help countries that do not have a CSIRT in place, in accordance with ENISA.[36]

5.4 What role for the European Union?

The efforts made by various institutions of the European Union against cyber-crime can be placed into four categories. The first is a legislative process, where the laws of the member states are harmonized because of the cross-border nature of cyber-crimes. This is for instance done with the aid of the Council of Europe Convention on Cybercrime (first referred to in the UN section above). The second category is the enhancement of inter-governmental cooperation in law enforcement. This is for instance done by establishing points of contact in every member state but also by providing an EU platform to train cyber-crime experts. The third category revolves around public-private partnerships, most importantly between law enforcement agents and private companies. With many incidents still going un-reported, the sharing of information across public/private as well as inter-state lines needs to be reinforced. The fourth category involves wider international cooperation against cyber-crimes, since the crimes do not end at the EU borders, and therefore it is clear that an international effort is required (European Commission, 2008).

In October 2009, during Sweden's six-month Presidency of the EU Council, the 'Stockholm Programme' was presented as an effort to build an open and secure Europe that would serve and protect its citizens (Council of the European Union, 2009).[37] Focussing on the broad area of internal security, law and justice, the programme calls for improvements in many fields including in the fight against racism and xenophobia (p. 15), the sharing of tools and information (p. 37), cross-border law enforcement (p. 40), increasing the role of Europol as a intermediary between cooperating nations (p. 41), combating serious and

[36] ENISA stands for European Network and Information Security Agency. It works on behalf of EU member states and institutions as a 'pacemaker' for Information security in Europe. URL: http://www.enisa.europa.eu/

[37] Report is available at URL: http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf

organized crimes (p. 43), fighting child pornography (p. 46), terrorism (p. 50), and lastly fighting cyber-crimes (p. 47). Not only this last issue but all the other aspects mentioned could fall into the cyber-paradigm to some extent. The programme stresses that member states should sign and bring into force the 2001 CoE Convention on Cybercrime. Under the Convention Europol could provide a central point for member states to share best practices, but information should also be shared with states outside the EU (p. 47). The European Commission is to work on enhancing the partnership between private and public actors, with a view especially to fighting the proliferation of child pornography. The EU also wants to intensify cooperative effort between the Council, the Commission, the Parliament and the Member States to promote higher levels of network security and to promote faster awareness and reaction in the case of a cyber-attack within the Union (p. 39).

Like NATO, the European Union has been working for some time on diverse aspects of CEP and civil emergency response, and in February 2010 – as a consequence of the Lisbon treaty – raised cooperation to a new level by creating the new Standing Committee on Internal Security (COSI) (The Spanish Presidency of the European Union, 2010). COSI is designed to enhance cooperation in important law enforcement areas such as terrorism, human trafficking, drug trafficking and cyber-crimes. Its first task is to evaluate the operational cooperation between member states and offer suggestions on how weaknesses can be mended. COSI is also to make recommendations on an early warning system regarding CRBN weapons, the creation of support teams for major terrorist attacks, and improving the system to locate high-risk missing persons. It is also to coordinate the efforts of the various European law-enforcement agencies such as Eurojust and Europol so that there is less overlapping of efforts. Lastly the committee will look to enhance border control cooperation, for instance by enhancing the exchange of DNA data, finger-prints or vehicle information.

If the EU has not so far seemed prominent in the development of cyber-security as such, that may be partly because of the division of effort between many different lines and agents of EU policy, but also a lack of political emphasis and the fact that the EU organs and other states have not put such effort into

external cooperation – notably with the US - as the UK has. This extensive information and method sharing across the Atlantic has been very beneficial for the UK (Evans and Whittell, 2010). States like Estonia have also preferred to turn to NATO when they felt they were under serious attack. However, the EU's open internal space and its often turbulent external borders, as well as its members' generally high technological level and reliance on IT, make it a large and vulnerable target for cyber-attacks of all kinds. It remains to be seen whether the subject will rise higher on the EU's policy agenda as a result of the creation of COSI and other measures for intensifying internal security work under the Lisbon Treaty.

In the summer of 2009 Iceland applied for membership of the European Union and the European Commission issued its Opinion on Iceland's qualifications in February of 2010 (European Commission, 2010).[38] The EU determined that Iceland was a valid participant in international efforts as a member of the organizations mentioned in this chapter and many other international organizations and agreements, including regional ones such as the Arctic Council and the Council of Baltic Sea States. Because of all these efforts, Iceland should be ready for full and active participation in the Common Foreign and Security Policy and European Security and Defence Policy.[39]

In the case of an Icelandic accession to the Union, Iceland would become part of all EU policies, committees and other bodies dealing with internal security and CEP, and a full member of Europol and Eurojust (where it has a liaison relationship at present), on top of its existing membership of Schengen. The real-life impact on issues like cyber-security is difficult to assess. Since Iceland is an island unconnected to any other European nation there are no shared infrastructures and no domino-effect dangers that need to be avoided, so Iceland would probably continue handling most of its own infrastructural security. At the same time the European Union would be very helpful in terms of cooperation between Member States and their law enforcements agencies on the one hand, and Iceland on the other hand. Iceland has been a participant in the European

[38]Report is available at URL:
http://ec.europa.eu/enlargement/pdf/key_documents/2010/is_opinion_analytical-report.pdf
[39] The EU website on Iceland can found at URL:
http://ec.europa.eu/enlargement/press_corner/key-documents/opinion-iceland_2010_en.htm

Commissions Humanitarian Aid and Civil Protection. Iceland is a participant in the Community Mechanism which is aimed at enhancing cooperation in civil protection matters. Since time is often of great importance in the case of disasters, the Mechanism has the tools to make coordination and flexibility more effective. (European Commission, n.d) Iceland will also be covered by the 'solidarity' clause in Article 222 of the Lisbon Treaty, making the cooperation more official, obliging all members to assist each other in the event of major damage from terrorist attacks and natural disasters (Council of the European Union, 2008). In principle this range of options could also be used for emergencies that began in or seriously affected Iceland's critical information infrastructure.

5.5 Europol

As Iceland already has access to cooperation with Europol and the latter has focussed explicitly on cyber-crimes, it will be covered in more detail here. Europol works as the law enforcement agency of the EU, and handles the pooling and exchange of criminal intelligence to prevent and combat serious international organized crime and terrorism. The aim of Europol is to make a difference in the fight against organized crime, and that difference is best achieved by targeting the criminal organizations (Europol, n.d). Europol has no executive for instance to perform arrests, but instead works as an information hub and advisory body. It publishes reports regarding the latest threats and makes crime analysis based on information from Member States and from other sources. Europol also handles training, coordination and expertise, as well as technical support in operations performed within the European Union. These operations are always under the authority and responsibility of the relevant Member State. Europol's tools can make a valuable difference when it comes to the fight against transnational organized units.

Europol works with Member States on specific law enforcement activities, of which the ones most relevant to this thesis are the fight against terrorism, trafficking of human beings (including child pornography), money laundering, crimes against individuals, financial crimes and lastly cybercrimes. Europol can be called on for assistance when serious crimes, acts of terrorism or organized crime units have had effects in two or more Member States. In later years the requirement for crimes to be committed by a 'group' has been relaxed somewhat,

given the way that serial killers for instance can move rather freely within the EEA. Europol has also been active in harmonizing certain techniques within the Member States, thus making international cooperation easier. Europol cannot investigate crimes on its own, but must either wait for an official request from a Member State or request a Member State to look into specific matters. Europol has at its disposal not only regular law enforcement officers but also various specialists from various fields, such as financial police, border matters and customs. Language barriers can be an obstacle in international cooperation, but the aid of Europol can help to avoid that.

Decisions by the Justice and Home Affairs Council of the EU have made it possible for Europol to enter into cooperation with both international bodies not connected with the EU, and states that are not Member States of the European Union. There are two types of cooperation treaties that can be signed, a strategic agreement that is limited to exchange of non-personal data, and operational agreements that include possible exchange of personal data. This means that when a person is sought through the Europol area, that person can be named. Iceland currently has an operational agreement with Europol (Europol, 2001)[40], signed in 2001 and facilitated by the fact that Iceland is also part of Schengen cooperation, the EEA and the Nordic law enforcement cooperation. The agreement between Iceland and Europol applies to drug-trafficking, trafficking of nuclear and radioactive substances, the trade and smuggling of human beings, motor vehicle crimes, possible terrorist attacks and money forgery and laundering.

Europol set up a special 'Analysis Work File' named ‘Cyborg’ on Cyber-crime after many member states reported an increase in cyber-crimes (Quillé, 2009).[41] Europol rightly figured that cyber-crimes are international for the most part and therefore a cross-border approach was more fitting than an ad hoc approach. The Work File will focus among other things on Internet-related organized crime, such as computer intrusion fraud. The crimes that the Work File will focus on are defined in the Convention on Cybercrime published by the

[40] Document is available at URL:
http://www.europol.europa.eu/legal/agreements/Agreements/9678.pdf
[41] Document is available at URL:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/IF_2009_presentations/2079if09pres_quille_europol.pdf

Council of Europe. To quote from Europol's High Tech Crime Threat Assessment from 2007: 'The Council of Europe is one of the main actors and points of force in fighting HTC' (Europol, 2007). The CoE's Octopus programme, discussed in more detail below, offers a firm framework for many stakeholders to cooperate in discussing and implementing the Cybercrime Convention, which is due to be ratified by additional countries in the next months. As Europol notes, this will finally give a wide range of states 'a common legal platform, whose lack has been one of the main hurdles in fighting HTC' (Europol, 2007).

5.6 Council of Europe

The Council of Europe (CoE) was founded in 1949 by 10 members in the wake of the Second World War. At the time it represented the first attempt, backed by the US and UK, to create a united Europe with a single 'phone number', but its importance was soon diminished by the rise of the European Communities, NATO and CSCE/OSCE. At present the CoE consists of 47 members, i.e. every European state except Belarus and Kazakhstan. The primary goal of the CoE has been to safeguard the rights and dignity of the people of Europe by upholding three fundamental values, democracy, human rights and the rule of law, which the CoE sees as cornerstones of a well functioning Europe that can grow together without internal disputes. These values also dictate the CoE's interest and engagement in the fight against threats such as terrorism, corruption, violence against children and women, human trafficking and cybercrimes, to name only a few security-relevant examples (Council of Europe, n.d). The main way the Council of Europe operates is to draft legally binding international conventions that are designed to bring the laws of the member states closer together than would otherwise be the case. These conventions number more than 200 at present, with the best known probably being the European Convention on Human Rights. That convention places certain obligations on the member states regarding the rights and freedoms of individuals within their jurisdictions. CoE conventions are supplemented by resolutions and recommendations by the member states, seeking mutual solutions to the many common problems of modern society (Council of Europe, n.d).

The Council of Europe has been focusing on cybercrime for a longer time than most other international organizations, and even longer than many states. The

Convention on Cybercrimes was adopted in 2001 and came into force in 2004, after being signed and ratified by 15 states (The Council of Europe, 2001).[42] Iceland signed the convention in 2001, but it did not come into force until 2007. In 2007 the Council of Europe held its first Octopus Interface conference, bringing together specialists from every part of the world, with the aims of promoting the Convention on Cybercrime and its guidelines and encouraging further ratifications. More generally the conferences, repeated annually since 2007, give specialists a chance to meet and find out what is going on in the business (The Council of Europe, 2007). The attendance has risen from 140 people in 2007 to around 300 in 2009, coming from over 70 countries, international agencies and the private sector. As of 2010, no one from Iceland is on a list of participators.

The Council has also adopted guidelines for states on how cooperation between law enforcement agencies and Internet Service Providers (ISPs) should be conducted in the fight against cyber-crimes (The Council of Europe, 2008).[43] As has been stated before, working against crime in cooperation with ISPs can be difficult because of their responsibilities to their customers. Even if the companies were willing to violate any possible trust, the matter could still fall under international agreements on human rights and so on. This is a reason why an international convention on this cooperation is very important. The CoE guidelines for instance call for good information sharing between both sides, which should have specific contact points for the cooperation manned by trained professionals. Any requests made by either side should be kept formal, so that no information is released to unauthorized individuals. Law enforcement officials should share as much information as possible with the ISPs, without putting at risk any possible future or present investigations, to make clear the importance of what the ISPs can add. The ISPs for their part are asked to report any crimes that they might witness without actually trying to pursue them, and are also asked to help in training for law enforcement officials. It is clear that if these guidelines would be followed by all ISPs and all law enforcement agencies, the fight against cyber-crimes would certainly be more successful (The Council of Europe, 2008).

[42] Convention is available at URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[43] More on this project can be found at URL: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

There are also projects ongoing in the Council of Europe regarding Cloud Computing, seen as an application on the verge of rapid expansion. A very simple example would be a Google Mail account that can be accessed from anywhere in the world, but where the data is not held on a personal or institutional server and is not easy to localize. Rather, it is stored by the network providers in data centres all around the world, and there are projects underway to establish data centres in Iceland. There are several problems that can arise when it comes to cloud-computing, such as full disclosure in the case of infiltration and profiling where private data is examined for commercial gains (Jensdóttir, 2010). Developing safety protocols for this field offers opportunities for countries that might be willing to participate in international efforts, and could for instance be an interesting point for Iceland to look into, especially when it comes to possible data centres in Iceland.

5.7 Interpol

As is clearly seen in this chapter, there is a large international effort to fight cyber-threats, with many international bodies exploring different aspects of cyber-crime. A special department of Interpol works on Financial and High-Tech crimes, which involve counterfeiting, money laundering, credit card fraud, cyber-attacks and cyber-terrorism - all aspects of the same spectrum, as discussed above. As early as in 2006 the General Assembly of Interpol recognized that there was an urgent need to raise cyber-crime awareness amongst individuals, but also within law-enforcement personnel, governments and private industry, along with harmonizing global training initiatives and supporting the development of law enforcement (Interpol, 2006).

The efforts of Interpol can be divided into three categories, information exchange, investigation capabilities and regional working parties (González, n.d). Information is exchanged through the Interpol website and the Interpol Criminal System, which has established various procedures and points of contact in other countries. The investigation capabilities are enhanced through training in various fields such as advanced computer learning and other relevant field skills, but also with manuals published by Interpol and videos made by the organization. Interpol has divided the world into four regions (Asia-South Pacific, Africa, Europe and North-America/Middle-East) where groups have been formed, and these groups

cooperate by sharing information and practical experience, promoting the standardization of methods used and establishing guidelines on good practices. Interpol's future aims in fighting cyber-threats will mainly be focused on enhancing this regional cooperation so that the organization can truly be called international, working to create an international standard on investigative and information exchange issues, and lastly building effective partnerships that will improve efficiency and response ability (Interpol, n.d).

5.8 International cooperation between CERT groups

There are many different types of CERT groups, focussing on security for different networks. The main types are Academic, Commercial, Governmental sector, military sector and a national type. Iceland has an academic CERT group and a military sector CERT team, but – as discussed in the last chapter - other fields are still not covered. Other comparable institutions include WARP groups (Warning, Advice and Reporting Points) which have been established i.a. in the UK to protect the country's infrastructure from infrastructural attacks by enhancing the sharing of information on alerts and warnings, improving awareness and education, and encouraging the reporting of incidents to the proper agencies. WARPs cooperate with the business community and other important actors to reduce the risk to their organizations (ENISA, 2006, p. 10).

CERT groups can of course be linked internationally, and examples involving Iceland include NORDUNet, where RHNet handles the relationship. NORDUNet is a network of Scandinavian CERT teams that focus on research networks. RHNet is focused on the Icelandic university network, working on enhancing the communications between the networks in Iceland (RHNet, n.d). It does not handle individuals. The network for the Icelandic Defence Agency is handled by what could be called a military CERT team, in accordance with NATO standards.

Cooperation between CERTs within regions has been seen to be very effective. The examples for this are several, but the main ones would be in Asia and Europe. The APCERT (Asia-Pacific CERT) was established in 2003 under pressure from Japan's CERT team. The APCERT gave itself several goals to achieve, including maintaining a trusted network of experts in the Asia Pacific

region that would work to raise awareness and competence in the field of computer security. The group also aimed at improving the contribution from the Asia Pacific region in international computer security efforts, by working together on research in the field and sharing information among members and with other CERT teams that might be need of experience. Finally the group wanted to take a stand on the legal issues regarding computer security and emergency responses across boundaries (ENISA, 2006, pp. 21-22). A similar European example would be the European Government CERT-group, established in 2007 and including Norway's, Sweden's and Finland's governmental CERT teams, along with Germany, France and the UK (ENISA, 2006, p. 16).[44] The Nordic countries' teams in this network are different from the academic CERTs who are members of NORDUNet, The cooperation is based on the similarities between the societies of these countries and their challenges, and the aims are to improve defences against large-scale or regional security incidents, facilitate information sharing related to security measures, identify fields where knowledge and expertise can be shared between members, and encourage the formation of government CERT teams in other European countries.

Since it can be said that an establishment of a CERT team is a benefit for everyone except the criminals, information on how to set up a CERT team is widely available (Carnegie Mellon Software Engineering Institute, 2004).[45] The benefits of setting up such a group include providing a trusted point of contact within a country, and an organization that can make contingency plans for all sorts of incidents within the borders of the country involving all known threats. The organization then also conducts threat analysis and evaluates vulnerabilities and shares information with the appropriate stakeholders. It can help other agencies in the country to develop their own capabilities so that they can respond to any threats that might occur, inter alia by making available educational material suitable for all levels of knowledge from the company leader to the traditional Internet user. National CERT's are also the Points of contact for foreign CERT teams and regional groups. The most important asset for a CERT team, as with other protection agencies, is the trust of the people it is designed to protect. If the

[44]This group can be examined further at URL: http://www.egc-group.org/
[45] The report is available at URL: http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

constituency does not trust the protector, and fails to seek protection, the threats wil[l] continue.

5.9 Conclusions

It is clear that the possibilities for cooperation when it comes to cyber-threats are extensive, and most of them are available to the Icelandic government if it so chooses. Even within Iceland's regional space the opportunities are varied and do not require substantial funding. The most important thing needed from Iceland's side would be compliance with the standards used in international operations. By upholding these standards Iceland would easily be able to participate in international efforts and receive assistance from international bodies in setting up security organizations within the country. Iceland is already a member of most of the organizations mentioned in this chapter and many of them have common funds to pay for many of the available tools, minimizing the need for extra national funding. In any case there is no easy answer – in this case or others – to the question of how the security of the people should be price-tagged.

The opportunities are in fact even more varied than indicated in this chapter. To give just one further example, the OSCE, of which Iceland has been a member for many years, has been training police officers in Kosovo to be better able to respond to cyber-threats such as identity theft, credit card fraud and money laundering. The most important problems the Kosovo police encountered are legislation issues and language problems, and since cyber-crimes are transnational it is important that laws are compatible and language barriers do not hinder prosecutions (Sopa, 2010). If Iceland should be interested in similar help and since costs are paramount, it should be mentioned that OSCE missions are most often funded by the Unified Budget. Sometimes the beneficiary country has participated in the cost of the respective project but most often the OSCE covers the entire cost (Zavisic, 2010). While other international institutions might at some time tried to aid participants when it comes to travel costs, an international crisis does not go unnoticed by international agencies, and so aid has been cut in some cases (Bartholin, 2010).

There is also another broader international argument that could be taken into consideration. Vilborg Ása Guðjónsdóttir asserted in her MA thesis that one

of the reasons for the rift between the US and Europe in recent years is because of a lack of a common threat, and that theme can be found in many other recent analyses (Guðjónsdóttir, 2009). Before that rift there was of course the common threat of the Soviet Union, which united many nations and people that would otherwise be enemies. In this new globalized world there are many transnational threats, be it organized crime, environmental threats or cyber-threats, and all of these need transnational cooperation for greatest effectiveness. International efforts for cyber-security seem bound to grow and if European and Northern American nations could take a lead in this process together, a bonus effect could possibly be a mending of the rift that has plagued the world for the better part of two decades.

6. Conclusions

Throughout this thesis there are certain ideas that have recurred, put forward both by international organizations and individuals in the public and private sector to help states and societies combat cyber-threats. Cooperation is a large part of the suggested remedies, and this is all the more important as an issue for Iceland. In more senses than one, cooperation has not been the 'Icelandic way', either in the international arena or when it comes to internal matters. Everyone agrees that this needs to be fixed, but the actual task seems to be hard. The situation in Iceland regarding cyber-security clearly presents the opportunity to make an attempt, thanks to the small number of experts and very similar infrastructural systems. The only factor needed is the will.

The smallness of the country and the infrastructure is often said to be a hindrance for guaranteeing security, but in this case it does not have to be the case. In many other countries the military would handle this type of defence but that is not possible in the case of Iceland, and therefore the matter needs to be handled in a different way. Given that there are few 'specialists' and that real diversity across the country is minimal, the same medicine could work for the entire nation. Measures intended for the people can reach them without significant trouble, building the required trust. The smallness of the country could also make Iceland valuable on the international scene, offering impartiality that can often be beneficial when larger entities come together to discuss international matters. If an international agreement on the use of cyber-weapons is to be made possible - for example - nations such as China and Russia need to come to the table. They might be more willing to come at the request of little Iceland rather than the larger US, to name one example.

China and Russia both have certain image problems that can be hard to fix. China has become an easy scapegoat when it comes to cyber-attacks, but China also has internal cyber-problems. The same can be said about Russia. These

nations, along with others in similar situations, could be unwilling to enter into international agreements on a basis where they are seen as the culprits. A better understanding is needed throughout the international arena on the particularities of cyber-attacks, notably on how easily the origins of the attack can be manipulated. Even when all evidence points in one direction, no guilt should be assumed when it comes to cyber-attacks. This would then clarify that in fact all states in the system are possible victims, and need to focus on cyber-matters together.

It can be seen that there are some similarities between the international and the local sphere when it comes to cyber-security. Information for all concerned parties is a foundation for the future, and this applies inside Iceland as well as outside. It should be mentioned that the battle is somewhat biased in that security is commonly considered boring, that is that no one really wants to sit down after a long day and learn about security, and this has been named as a reason for the lack of a security-mentality in Iceland (Skúlason & Finnbogason, 2010). In return it can be pointed out that it took an initiative to pass legislation in the matter of safety belts for the mentality to sink in, and that is perhaps what would be needed in this case as well. Safety belts have become a habit that can be learned by all, and that could perhaps also be done in the case of cyber-security.

Based on the analysis above, this is a list of possible future actions that should be undertaken in Iceland for the sake of cyber-security:

1. The first step is to establish a CSIRT team or some entity with similar function. That team should be situated within the government, as per the recommendations of the report covered in section 4.2.1. Enlisting the help of experts within the Icelandic community is also a valuable step. They would help in determining what is needed in terms of personnel and hardware, and could help provide the public trust needed for this measure to be successful.

2. The government should carry out an updated threat assessment, determining what Iceland's weak points are, but also what the strengths are. This should be done in cooperation with the experts from the first step, but also with the private sector more generally.

3. Establish a connection with other international actors working in this field. The other Nordic countries would be a clear start, as well as existing NATO connections. They could provide links to other agencies that should be contacted.

4. Take steps to publicize the progress made, so that everyone knows that Iceland is now fully protected against any type of threat.

5. Ordinary people in Iceland need to know that they have a role in the fight against cyber-threats. As was seen in the Council of Europe Convention on cooperation with ISPs, the ISPs need as much information as possible in order to keep the cooperation on-going. The same applies with the general public, who needs to know that their small contribution to the security of the state is worthwhile, and also that they cannot depend on someone else to protect them. There is no subject more fitting than one of the greatest threats the modern world has faced for Icelandic society to start focusing on its own security.

6. Finally when matters have been handled as well as can be expected domestically, it is time to look abroad. Iceland's small but tight expert core could be very helpful for other countries, and could provide valuable information about the establishment of a contingency centre that could handle everything from a natural disaster to a cyber-attack.

This thesis has been somewhat pessimistic about the security situation in Iceland, and it may very well be that the true situation is better than described here. But the fact remains that if no information on effective security measures is available, it has to be assumed that the country is ill-defended. For a long time discussions on Icelandic defence (or lack thereof) have been something of a taboo, meaning that the matter should not be discussed in any detail. Maybe a declaration to the effect that Iceland is now secure – as proposed above - would only raise the country's profile and make a larger target of Iceland. But making and announcing improvements must be better than remaining un-defended and simply hoping that no one stumbles upon the fact. Any joy that a hacker finds in destroying a website

would certainly be multiplied in destroying a whole country. In any case, this thesis has found some brighter spots to be mentioned, with the National Police Commissioner leading the way for the rest of the country. Every ministry and institution in Iceland has had to cut its budget lately, with most of them barely keeping their heads above water. Progress, coordination and international cooperation under those circumstances can offer maximum value.

Iceland has for the most part been a passive participant in international efforts. This has been explained by the small-state mentality and the view that a small player cannot make any real difference, but it has also been assumed that the country is self-sufficient in most ways. While that may be true in some specific respects, it is clear that in this closely connected world no country is really an island, and that fact offers positive openings as well as risks. Iceland has a possibility to find a niche for itself in the high-tech industry, for instance with the establishment of data-centres depending on cheap clean energy. When Iceland has solved its domestic problems there is no hindrance to Iceland's finally becoming a valuable member of the international system, for instance by offering expert assistance on cyber-security when it comes to legislation and technical matters. Iceland’s smallness does not need to be a hindrance, as the smallness can increase the flow of information and make the national expert team more efficient and better able to deal with larger-scale issues. Any international efforts that Iceland would participate in would then also bring more knowledge back to the country, keeping Iceland in the forefront of the field. The first step towards all of this is still to realize that there is a problem in the country today and to successfully fix these problems. Without that step any build-up of international links would be based on a rotten foundation and be susceptible to fall at any moment. It is the expressed wish of the author that Iceland has learned its lesson in this regard.

Bibliography

Areddy, J. T. (2010, February 18). *People's Republic of Hacking.* Retrieved March 6, 2010, from The Wall Street Journal: http://online.wsj.com/article/SB10001424052748704140104575057490343183782.html?mod=WSJEUROPE_newsreel_technology

Arnþórsson, H. (2010, March 23). Regarding electronic governance. (J. K. Ragnarsson, Interviewer)

Bailes, A. (2010). *Does a small state need a strategy?* Retrieved April 1, 2010, from Alþjóðamálastofnun: http://stofnanir.hi.is/ams/sites/files/ams/Bailes_Final_0.pdf

Bailes, A. (2007). Introduction: A World of Risk. In SIPRI, *SIPRI Yearbook 2007.* Oxford: Oxford University Press.

Bailes, A. (2009). Security in the Twenty-First Century. In A. Bailes, *Through European Eyes* (pp. 3-13). Reykjavík: University of Iceland Press.

Bartholin, K. (2010, April 12). Council of Europe Criminal Law Division (Conducted via email). (J. K. Ragnarsson, Interviewer)

Bartz, D., & Finkle, J. (2009, November 24). *Cyber breaches are a closely kept secret.* Retrieved February 9, 2010, from Reuters: http://www.reuters.com/article/idUSTRE5AN4YH20091124

BBC News. (2010, March 21). *Volcano erupts in south Iceland.* Retrieved March 30, 2010, from BBC News: http://news.bbc.co.uk/2/hi/europe/8578576.stm

Blair, D. (2010). Annual Threat Assessment of the US Intelligence Community. *The House Permanent Select Committee on Intelligence.* Washington: US House of Representatives.

Blakely, R., Richards, J., & Halpin, T. (2007, November 2007). *Cybergang raises fear of new crime wave.* Retrieved January 15, 2010, from TimesOnline: http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2844031.ece

Boessenkool, A. (2010, February 2). *NATO Chief: Nations Must Unite On Cyber Warfare.* Retrieved March 6, 2010, from Defense News: http://www.defensenews.com/story.php?i=4483043&c=EUR&s=TOP

Bosch, O. (2004). Defending against cyber-terrorism: preserving the legitimate economy. In A. Bailes, & I. Frommelt, *Business and Security: Public - Private sector relationships in a new security environment* (pp. 187-197). Oxford: Oxford University Press.

Bradbury, D. (2009, February 5). *The Fog of Cyberwar.* Retrieved February 10, 2010, from guardian.co.uk: http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access

Branigan, T. (2010, February 8). *China closes training website for hackers.* Retrieved March 3, 2010, from guardian.co.uk: http://www.guardian.co.uk/world/2010/feb/08/china-closes-hacking-website

Brewin, B. (2009, November 20). *Electronic Health records could be a deadly target during a cyberwar.* Retrieved February 15, 2010, from nextgov: http://www.nextgov.com/nextgov/ng_20091120_8634.php?oref=topstory

Bristow, M. (2009, June 9). *China defends screening software.* Retrieved March 4, 2010, from BBC News: http://news.bbc.co.uk/2/hi/asia-pacific/8091044.stm

Bronk, C. (2009, August 13). *Time to move toward a more secure Cyberspace.* Retrieved January 23, 2010, from World Politics Review: http://www.worldpoliticsreview.com/article.aspx?id=4194

Bronk, C. (2010, January 19). *Towards Cyber Arms Control with Russia.* Retrieved February 19, 2010, from World Politics Review: http://www.worldpoliticsreview.com/article.aspx?id=4959

Bæjarins Besta. (2009, December 3). *Rafmagnstruflanir á Vestfjörðum [Electrical disturbance in West Fjords]*. Retrieved January 15, 2010, from Bæjarins Besta: http://www.bb.is/?PageID=26&NewsID=141301

Böðvarsson, E. (2010, March 29). Skýrr. (J. K. Ragnarsson, Interviewer)

Cantrell, T. (2010, April 14). CTO at Verne Global. Conducted via email. (J. K. Ragnarsson, Interviewer)

Carnegie Mellon Software Engineering Institute. (2004). *Steps for creating National CSIRTs* . Pittsburgh: Carnegie Mellon University.

Carr, J. (2007, December 18). *Finjan: Chinese cybercrime networks fill void left by Russian Business Network.* Retrieved January 7, 2010, from SC Magazine: http://www.scmagazineus.com/finjan-chinese-cybercrime-networks-fill-void-left-by-russian-business-network/article/100002/

CCD-COE. (2008). *CCD-COE Report.* Tallinn: Cooperative Cyber Defence Centre of Excellence.

CCD-COE. (2010, January 11). *Symantec and Cyber Defence Centre of Excellence Experts to Research Online Threats.* Retrieved April 15, 2010, from CCDCOE News: http://www.ccdcoe.org/162.html

Center for Strategic and International Studies. (2008). *Threats Posed by the Internet.* Commission on Cyber-security for the 44th President.

Clarke, R. (2002). Administrative Oversight: Are we ready for a cyber-terror attack? *Senate Committee on the Judiciary Subcommittee on Administrative Oversight and the Courts.* Washington: US Senate.

Connolly, K. (2009, Juky 22). *Germany accuses China of industrial espionage.* Retrieved March 15, 2010, from guardian.co.uk: http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage

Cornish, P., Hughes, R., & Livingstone, D. (209). *CyberSpace and the National Security of the United Kingdom.* London: Chatham House.

Council of Europe. (n.d). *The Council of Europe: Who we are - What we do.* Strasbourg: Council of Europe

Council of Europe. (2001). *Convention on Cybercrime.* Budapest: The Council of Europe.

Council of Europe. (2007). *Octopus Interface 2007.* Retrieved January 26, 2010, from Council of Europe: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp

Council of Europe. (2008). *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime.* Strasbourg: The Council of Europe.

Council of Europe. (2008). *Cybercrime: Current threats and trends.* Strasbourg: Council of Europe.

Council of the European Union. (2008). *The Lisbon Treaty.* Brussels: Council of the European Union.

Council of the European Union. (2009). *The Stockholm Programme – An open and secure Europe serving and protecting the citizens.* Brussels: The Presidency of the Council of the European Union.

Davies, C. (2010, January 14). *Welcome to DarkMarket - global one-stop shop for cybercrime and banking fraud.* Retrieved February 15, 2010, from guardian.co.uk: http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley

Dunn-Cavelty, M. (2007). Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics Vol. 4(1)* , 19-36.

Elegant, S. (2009, November 18). *Cyberwarfare: The Issue China Won't Touch.* Retrieved January 9, 2010, from Time.com: http://www.time.com/time/world/article/0,8599,1940009,00.html

Elegant, S. (2007, December 6). *Enemies at the Firewall.* Retrieved January 6, 2010, from time.com: http://www.time.com/time/magazine/article/0,9171,1692063,00.html

ENISA. (2006). *CERT cooperation and its further facilitation by relevant stakeholders.* Crete: ENISA.

ENISA. (n.d). *NCIRC NATO Cyber Defense Workshops*. Retrieved March 15, 2010, from ENISA: http://www.enisa.europa.eu/act/cert/background/inv/initiatives-outside-europe/ncirc

Epstein, J. M. (2009, August 6). *Modelling to contain Pandemics.* Retrieved February 17, 2010, from nature.com: http://www.nature.com/nature/journal/v460/n7256/full/460687a.html

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, security and international relations: (IR)Relevant Theory? *International Political Science Review 27*, 221-244.

Eshel, D. (2010, March 15). *Killer Apps.* Retrieved March 20, 2010, from Aviation Week: http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/dti/2010/02/01/DT_02_01_2010_p39-198440.xml&headline=Israel%20Adds%20Cyber-Attack%20to%20IDF

Espiner, T. (2008, December 10). *Experts spilt over recession's effect on high-tech crime.* Retrieved January 9, 2010, from ZDNet UK: http://www.zdnet.co.uk/news/security-threats/2008/12/10/experts-split-over-recessions-effect-on-hi-tech-crime-39574471/

Espiner, T. (2007, November 9). *Infamous Russian malware gang vanishes.* Retrieved January 6, 2010, from cnet.news: http://news.cnet.com/Infamous-Russian-malware-gang-vanishes/2100-7355_3-6217852.html

European Commission. (2010). *Commission Opinion on Iceland's application for membership of the European Union.* Brussels: European Commission.

European Commission. (2009). Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the committee of the regions. *Impact Assessment (part 1).* Brussels: Commission of the European Communities.

European Commission. (2008, July). *Fight against cyber crime*. Retrieved April 8, 2010, from Freedom, Security and Justice:

http://ec.europa.eu/justice_home/fsj/crime/cybercrime/wai/fsj_crime_cybercrime_en.htm

European Commission. (n.d). *The Community mechanism for civil protection*. Retrieved April 5, 2010, from European Civil Protection: http://ec.europa.eu/echo/civil_protection/civil/prote/mechanism.htm#infopt1

Europol. (2001). *Agreement between the Republic of Iceland and the European Police Office.* The Hague: Europol.

Europol. (2009). *EU Terrorism Situation and Trend Report.* The Hague: Europol Corporate Communications.

Europol. (n.d). *Frequently Asked Questions*. Retrieved April 5, 2010, from Europol: http://www.europol.europa.eu/index.asp?page=faq

Europol. (2007). *HTCC Threat Assessment 2007.* The Hague: Europol High Tech Crime Center.

Evans, M., & Whittell, G. (2010, March 10). *Cyberwar declared as China hunts for the West's intelligence secrets.* Retrieved March 20, 2010, from TimesOnline: http://technology.timesonline.co.uk/tol/news/tech_and_web/article7053254.ece

Foreign Ministry of Iceland. (2009). *Áhættumatsskýrsla fyrir Ísland (Threat Assessment for Iceland).* Reykjavík: Utanríkisráðuneytið.

Goldirova, R. (2008, May 15). *NATO picks Estonia for high-tech crime centre.* Retrieved March 3, 2010, from euorserver.com: http://euobserver.com/9/26138

Goldsmith, J. (2010, February 1). *Can we stop the global cyber arms race?* Retrieved March 1, 2010, from The Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/31/AR2010013101834.html?hpid=opinionsbox1

González, S. T. (n.d). *Interpol's Role Fighting Cyber crime*. Retrieved April 3, 2010, from http://ispa.maz24.com/pdf-slides/isa06/gonzales.pdf

Gorman, S. (2009b, April 8). *Electricity Grid in U.S. Penetrated By Spies.* Retrieved March 8, 2010, from The Wall Street Journal: http://online.wsj.com/article/SB123914805204099085.html

Gorman, S. (2009a, August 17). *Hackers stole IDs for attacks.* Retrieved February 16, 2010, from The Wall Street Journal: http://online.wsj.com/article/SB125046431841935299.html

Guðjónsdóttir, V. Á. (2009). *The Future of Transatlantic Relations: Lessons from Disagreements between the United States and Europe from 1954-2009.* Reykjavík: MA ritgerð í alþjóðasamskiptum við Háskóla Íslands.

Habegger, B. (2008). Risk Analysis and Management in a Dynamic Risk Landscape. In B. Habegger. (ed.), *International Handbook on Risk Analysis and Management* (pp. 13-35). Zurich: Center for Security Studies.

Holahan, C. (2006, November 21). *The Dark Side of Second Life.* Retrieved January 16, 2010, from Bloomberg Business Week: http://www.businessweek.com/technology/content/nov2006/tc20061121_727243.htm

Hughes, R. (2009). NATO and Cyber Defence. *Atlantisch Perspectief: 2009nr1* .

Interpol. (2006). *Cyber-Criminality*. Retrieved January 18, 2010, from Interpol: http://www.interpol.int/Public/ICPO/GeneralAssembly/AGN75/resolutions/AGN75RES11.asp

Interpol. (n.d). *IT security and crime prevention methods*. Retrieved January 29, 2010, from Interpol: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp

Jenik, A. (April 2009). Cyberwar in Estonia and the Middle East. *Network Security Vol. 2009, Issue 4* , 4-6.

Jensdóttir, R. (2010, April 12). Council of Europe Secretary of the CDCJ. (J. K. Ragnarsson, Interviewer)

Johnson, B. (2009, December 22). *Russian hacker gang who 'stole millions from Citibank' under investigation.* Retrieved January 15, 2010, from guardian.co.uk: http://www.guardian.co.uk/technology/2009/dec/22/russian-hackers-citigroup-cyber-security

Karana, K. P., & Andriyanto, H. (2009, August 31). *Indonesian Hackers Claim Web Attack on Malaysian Sites*. Retrieved January 25, 2010, from Jakarta Globe: http://thejakartaglobe.com/home/indonesian-hackers-claim-web-attack-on-malaysian-sites/327111

Keizer, G. (2008, February 19). *Russian Hosting Network running a protection racket, resercher says.* Retrieved March 15, 2010, from Computerworld: http://www.computerworld.com/s/article/9063418/Russian_hosting_network_running_a_protection_racket_researcher_says

Kian, C. (2009, September 2). *Cyber Attacks on Malaysian websites*. Retrieved January 22, 2010, from F-Secure: http://www.f-secure.com/weblog/archives/00001760.html

Kingsbury, A., & Mulrine, A. (2009, November 18). *U.S. is Striking Back in the Global Cyberwar.* Retrieved March 16, 2010, from U.S. News: http://www.usnews.com/articles/news/2009/11/18/us-is-striking-back-in-the-global-cyberwar

Kolbeinsson, J. I. (2010, March 25). Kortaþjónustan. (J. K. Ragnarsson, Interviewer)

Krebs, B. (2007, October 13). *Shadowy Russian Firm seen as Conduit for Cybercrime.* Retrieved March 5, 2010, from The Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html

LaFraniere, S., & Ansfield, J. (2010, February 11). *China Alarmed by Security Threat From Internet.* Retrieved March 5, 2010, from The New York Times: http://www.nytimes.com/2010/02/12/world/asia/12cyberchina.html?scp=1&sq="center+for+strategic+and+international+studies"&st=nyt

Lambakis, S., Kiras, J., & Kolet, K. (2002). *Understanding "Asymmetric" Threats to the United States.* Fairfax: National Institute for Public Policy.

Lemon, S. (2007, March 28). *China Crafts Cyberweapons.* Retrieved January 15, 2010, from PCWorld: http://www.pcworld.com/article/132284/china_crafts_cyberweapons.html

Leyden, J. (2009a, October 23). *FBI and SOCA plot cybercrime smackdown.* Retrieved February 20, 2010, from SecurityFocus: http://www.securityfocus.com/news/11562

Leyden, J. (2009b, October 13). *Polish government cyberattack blamed on Russia.* Retrieved February 24, 2010, from The Register: http://www.theregister.co.uk/2009/10/13/poland_cyberattacks/

Loriaux, M. (1992). *The Realists and Saint Augustine: Skepticism, Psychology, and Moral Action in International Relations Thought.* In International Studies Quarterly, Vol. 36, No. 4(Dec, 1992), pp 401-420. Published by Blackwell Publishing.

Malik, M. A. (2010, January 17). *PEW advices banks to install extra layers of security.* Retrieved February 1, 2010, from The Daily Mail (Pakistan): http://dailymailnews.com/0110/18/CityPage/CityPages3.php

Mamatov, A. (2009, January 21). *Kyrgyzstan: government targets opposition.* Retrieved January 26, 2010, from EURASIANET.org: http://www.eurasianet.org/departments/insightb/articles/eav012109a.shtml#

McAfee Inc. (2005). *Virtual Criminology Report 2005.* Santa Clara: McAfee Inc.

McAfee Inc. (2009). *Virtual Criminology Report 2009.* Santa Clara: McAfee Inc.

McCarthy, K. (2010, February 17). *77% of domain registrations stuffed with rubbish.* Retrieved February 20, 2010, from The Register: http://www.theregister.co.uk/2010/02/17/domain_name_problems/

McMillan, R. (2008, August 15). *Anti-Georgia spammers building new botnet.* Retrieved March 2, 2010, from NetworkWorld: http://www.networkworld.com/news/2008/081508-anti-georgia-spammers-building-new.html

Menn, J. (2010, February 21). *US experts close in on Google hackers.* Retrieved March 21, 2010, from Financial Times.com: http://www.ft.com/cms/s/0/a6f5621c-1f21-11df-9584-00144feab49a.html?nclick_check=1

Miller, N. (2007, July 24). *From Russia with Malice: Criminals trawl the world.* Retrieved January 10, 2010, from theage.com.au: http://www.theage.com.au/news/business/from-russia-with-malice-criminals-trawl-the-world/2007/07/23/1185043032049.html

Mingst, K. (2004). *Essentials in International Relations.* London: W.W. Norton & Company, Ltd.

Ministry of Transport, Communications and Local Government of Iceland. (2008). *Stofnun forystu CSIRT/CERT teymis á Íslandi gegn öryggisatvikum í fjarskipta- og upplýsinganetum [On the establishment of an Icelandic CERT/CSIRT team for defence against incidents in communications and information networks]*. Reykjavík: The Post and Telecommunications Administration in Iceland

Ministry of Transport, Communications and Local Government of Iceland. (2009). *Umsagnir um stofnun CSIRT/CERT teymis á Íslandi gegn öryggisatvikum í fjarskipta- og upplýsinganetum [Review on the establishment of a CERT/CSIRT team against incidents in communications and information networks]*. Reykjavík: The Ministry of Transport, Communications and Local Government.

Morgunblaðið. (2010c, March 19). *Fjarskipti verði betur varin [Communications will be better guarded]*. Retrieved March 26, 2010, from Morgunblaðið: http://www.mbl.is/mm/frettir/forsida/2010/03/19/fjarskipti_verdi_betur_varin/

Morgunblaðið. (2004, May 5). *Grænfriðungar senda bréf til íslensks almennings [Greenpeace sends letters to Icelandic Public]*. Retrieved February 5, 2010, from Morgunblaðið: http://www.mbl.is/mm/frettir/innlent/2004/05/05/graenfridungar_senda_bref_til_islensks_almennings/

Morozov, E. (2009, April 11). *10 easy steps to writing the scariest cyberwarfare article ever.* Retrieved January 18, 2010, from Foreign Policy: http://neteffect.foreignpolicy.com/posts/2009/04/11/writing_the_scariest_article_about_cyberwarfare_in_10_easy_steps

NATO: Prague Summit. (2003). *The Prague Summit and NATO´s transformation.* Brussels: NATO.

NATO: Riga Summit. (2006). *Riga Summit Guide.* Brussels: NATO.

NATO: Bucharest Summit (2008). *Bucharest Declaration*, Section 47. Brussels: NATO.

NATO: Strasbourg/Kehl Summit (2009). *Strasbourg/Kehl Summit Declaration* (Section 49). Brussels: NATO.

NATO CEP. (2006). *NATO´s Role in Civil Emergency Planning.* Brussels: NATO.

NATO: *The North Atlantic Treaty of 4 April 1949.* Retrieved February 15, 2010, from NATO.int: http://www.nato.int/cps/en/natolive/official_texts_17120.htm

Neal, R. (2010, February 16). *Government is incapable of containing a large cyber attack, experts agree.* Retrieved March 2010, 2010, from Federal Times: http://www.federaltimes.com/article/20100216/DEPARTMENTS03/2160303/1001

Nisbet, C. (2003). *New Directions in Cyber-crime.* London: QinetiQ Ltd.

Nordic Council of Ministers. (2009). *The Nordic countries in figures 2009.* Copenhagen: Nordic Council of Ministers.

Norton-Taylor, R. (2007, September 5). *Titan Rain - How Chinese hackers targeted Whitehall.* Retrieved March 5, 2010, from guardian.co.uk: http://www.guardian.co.uk/technology/2007/sep/04/news.internet

Ólafsson, K. (2009). *Nordic Security Dynamics: Past, present - and future? MA ritgerð í alþjóðasamskiptum við Háskóla Íslands.*

Pétursson, J. I. (2010, April 9). At The National Commissioner for the Icelandic Police. (J. K. Ragnarsson, Interviewer)

Prime Minister's Office of Iceland. (n.d). *About island.is*. Retrieved March 3, 2010, from island.is: http://en.island.is/about-island-is/

Prime Minster's Office of Iceland. (2008). *Iceland the e-Nation: Icelandic Government Policy on the Information Society 2008-2012.* Reykjavík: Prime Minister's Office (Forsætisráðuneyti).

Quillé, M. (2009). *Key note address - Current threats and future challenges posed by cybercrime.* Strasbourg: Europol.

Reinart, V. (2009, October 22). *Lessons from the Estonian cyber-attacks.* Retrieved January 25, 2010, from NationalPost: http://network.nationalpost.com/NP/blogs/fullcomment/archive/2009/10/22/vaino-reinart-lessons-from-the-estonian-cyber-attacks.aspx

RHNet. (n.d). *RHnet -- Icelandic University Research Network*. Retrieved April 1, 2010, from RHNet: http://www.rhnet.is/english/

Rutherford, M. (2009, August 18). *Report: Russian Mob aided cyberattacks on Georgia.* Retrieved February 28, 2010, from Cnet News: http://news.cnet.com/8301-13639_3-10312708-42.html

Ruus, K. (2008, Winter/Spring). *Cyber War I: Estonia attacked from Russia.* Retrieved March 2, 2010, from The European Institute: http://www.europeaninstitute.org/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html

RÚV. (2010b, February 28). *Ekkert samband um Farice [No connection through Farice]*. Retrieved March 15, 2010, from RÚV: http://www.ruv.is/frett/ekkert-samband-um-farice

RÚV. (2010, January 31). *Rafmagnsbilun truflaði símasamband [Electrical malfunction interrupts telephone connections]*. Retrieved February 28, 2010, from RÚV: http://www.ruv.is/heim/frettir/frett/store64/item323085

Schwirtz, M., & Levy, C. (2009, June 23). *In Reversal, Kyrgyzstan Won't Close a U.S. Base*. Retrieved March 9, 2010, from The New York Times: http://www.nytimes.com/2009/06/24/world/asia/24base.html?_r=2&scp=24&sq=manas&st=cse

Shachtman, N. (2010, February 4). *'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google.* Retrieved March 4, 2010, from Wired.com: http://www.wired.com/dangerroom/2010/02/from-dont-be-evil-to-spy-on-everyone/

Sigurðardóttir, G. (2010, March 26). About the island.is project. (J. K. Ragnarsson, Interviewer)

Símonarsson, B. (2010, March 30). The Icelandic Defence Agency. (J. K. Ragnarsson, Interviewer)

Skúlason, F., & Finnbogason, F. Á. (2010, April 9). At Friðrik Skúlason ehf. (J. K. Ragnarsson, Interviewer)

Sopa, H. (2010, March 18). *OSCE trains Kosovo police in tackling cybercrime.* Retrieved March 28, 2010, from OSCE: http://www.osce.org/item/43136.html

Spanish Presidency of the European Union. (2010, March 11). *Recently created Standing Committee on Internal Security (COSI) begins its work.* Retrieved April 2, 2010, from Presidencia Espanola: http://www.eu2010.es/en/documentosynoticias/noticias/mar11_cosi.html

Stefánsson, S. S. (2009, December 4). (PTA) Conducted via email. (J. K. Ragnarsson, Interviewer)

Stefánsson, S. S. (2010a, March 11). (PTA) Conducted via email. (J. K. Ragnarsson, Interviewer)

Stefánsson, S. S. (2010b, March 16 and 17). (PTA) Conducted via email. (J. K. Ragnarsson, Interviewer)

Stefánsson, S. S. (2010c, January 12). (PTA) Conducted via email. (J. K. Ragnarsson, Interviewer)

Stefánsson, S. S. (2010d, March 11). (PTA) Conducted via email. (J. K. Ragnarsson, Interviewer)

Stefánsson, S. S. (2010, February 24). (PTA) Lecture on Security and Information, held by SKÝ. (J. K. Ragnarsson, Interviewer)

Stein, J. (2003). The Protean Enemy. *Foreign Affairs Vol. 82, No. 4(Jul-Aug)* , 27-40.

Stoltenberg, T. (2009). *Nordic Cooperation on Foreign and Security Policy.* Oslo: Ministry of Foreign Affairs of Norway.

Thompson, J. (2008, August 11). *"It still very difficult to get a call anywhere around the country right now."* Retrieved January 25, 2010, from Aid Worker Daily: http://aidworkerdaily.com/2008/08/11/it-still-very-difficult-to-get-a-call-anywhere-around-the-country-right-now-npr/

Thucydides. (2004). Melian Dialogue. In K. Mingst, & J. L. Snyder, *Essential Readings in World Politics* (pp. 18-20). London: W.W. Norton & Company, Ltd.

Traynor, I. (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia.* Retrieved March 3, 2010, from guardian.co.uk: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

Tully, A. (2009, September 16). *Intelligence Report Lists Russia, China as top U.S. Concerns.* Retrieved March 15, 2010, from Radio Free Europe Radio Liberty: http://www.rferl.org/content/Intelligence_Report_Lists_Russia_China_As_Top_US_Concerns_/1823807.html

UN Economic and Social Council. (2007). *Resolution 2007/20.* New York: United Nations Economic and Social Council.

UN General Assembly. (2003). *Resolution 57/239.* New York: United Nations General Assembly.

UN Security Council. (2001). *Resolution 1373.* New York: United Nations Security Council.

United Nations General Assembly. (1995). *Resolution 49/60.* New York: United Nations.

Urquhart, C. (2007, September 17). *Speculation flourishes over Israel's strike on Syria.* Retrieved March 15, 2010, from guardian.co.uk: http://www.guardian.co.uk/world/2007/sep/17/syria.israel

Vamosi, R. (2008, August 12). *Russia and Georgia continue attacks - online.* Retrieved February 26, 2010, from Cnet News Security: http://news.cnet.com/8301-1009_3-10015657-83.html?tag=nl.e703

Waltz, K. (1979). *Theory of International Politics.* Massachusetts: Addison-Wesley.

Warren, P. (2007, November 15). *Hunt for Russia's web criminals.* Retrieved February 8, 2010, from guardian.co.uk: http://www.guardian.co.uk/technology/2007/nov/15/news.crime

Weitz, R. (2009, August 25). *Global Insights: Russia Refines Cyber Warfare Strategies.* Retrieved March 1, 2010, from World Politics Review: http://www.worldpoliticsreview.com/article.aspx?id=4218

Wertsch, J. V., & Karumidze, Z. (2009). Spinning the past: Russian and Georgian accounts of the war of August 2008. *Memory Studies 2009; 2; 377* , 377-391.

West, M. (2010, February 15). *Online fraud costing £3.5 billion each year.* Retrieved February 20, 2010, from myfinances.co.uk: http://www.myfinances.co.uk/cut-your-bills/news/online-fraud-costing-3-5-billion-each-year-$1360307.htm

The White House. (2002, September). *National Security Strategy 2002.* Retrieved March 1, 2010, from The White House: http://www.globalsecurity.org/military/library/policy/national/nss-020920.pdf

Wikipedia. (2010, April 8). *Domain Name System*. Retrieved April 10, 2010, from Wikipedia.org: http://en.wikipedia.org/wiki/Domain_Name_System

Williams, R. (2007, November 29). *Global hackers threaten net security in cyber warfare aimed at top targets.* Retrieved February 18, 2010, from guardian.co.uk: http://www.guardian.co.uk/technology/2007/nov/29/hacking.news

Wæver, O. (1995). Securitization and de-securitization. In R. Lipschutz, *On Security* (pp. 46-86). New York: Columbia University Press.

Zavisic, D. (2010, March 23). Chief of Analysis and Reporting Cell, OSCE Mission in Kosovo. Conducted via email. (J. K. Ragnarsson, Interviewer)

Zetter, K. (2010c, February 4). *Google Asks NSA to Help Secure Its Network.* Retrieved March 4, 2010, from Wired.com: http://www.wired.com/threatlevel/2010/02/google-seeks-nsa-help/

Zetter, K. (2010a, January 14). *Google Hack Attack Was Ultra Sophisticated, New Details Show.* Retrieved February 10, 2010, from Wired.com: http://www.wired.com/threatlevel/2010/01/operation-aurora/

Zetter, K. (2010b, January 12). *Google to Stop Censoring Search Results in China After Hack Attack.* Retrieved February 16, 2010, from Wired.com: http://www.wired.com/threatlevel/2010/01/google-censorship-china/

List of Interviewees:

Alyson Bailes, University of Iceland
Arnar Jensson, Europol
Björn Símonarson, Icelandic Defence Agency
Chris De Wispelaere, NATO SPS
Dusko Zavisic, OSCE
Ebenezer Böðvarsson, Skýrr
Finnbogi Ásgeir Finnbogason, FRISK
Friðrik Skúlason, FRISK
Geir Ragnarsson, Ministry of Transport
Guðbjörg Sigurðardóttir, Island.is
Guðmundur Ingólfsson, Icelandic Defence Agency
Haukur Arnþórsson, Doctorate at the University of Iceland
Ingibjörg Rafnar Pétursdóttir, Foreign Ministry of Iceland
Jóhannes Ingi Kolbeinsson, Kortaþjónustan
Jón Ágúst Guðmundsson, MA at the University of Iceland
Jónas Ingi Pétursson, National Police Commissionner
Kristian Bartholin, Council of Europe
Kristmundur Ólafsson, CBSS,
Regína Jensdóttir, Council of Europe
Sigurður Darri Skúlason, Darval
Stefán Snorri Stefánsson, Post and Telecommunications Authority
Valur Ingimundarson, University of Iceland