Þjóðarspegillinn 2010

# Iceland and cyber-threats

Jón Kristinn Ragnarsson
Alyson J.K. Bailes

Stjórnmálafræðideild
Ritstjóri: Silja Bára Ómarsdóttir

Rannsóknir í félagsvísindum XI. Erindi flutt á ráðstefnu í október 2010

Ritstýrð grein

Reykjavík: Félagsvísindastofnun Háskóla Íslands

ISBN 978-9935-424-06-8

# Iceland and cyber-threats

Jón Kristinn Ragnarsson
Alyson J.K. Bailes

For the last twenty years the world has depended more and more on computers, for purposes ranging from the private and personal to the running of huge infrastructures and even military operations. But with added dependency comes added risk, and today cyber-threats are recognized as a major challenge for the twenty-first century. The great powers of the world and leading institutions are showing this in the emphasis they place on IT threats and cyber-security: NATO for instance has focussed on the topic since 2004 and even more after the cyber-attacks on Estonia in 2007. Cyber-threats are expected to play a clear part in the Alliance's forthcoming new Strategic Concept (NATO, 2010). At national level the same trend can be seen on both sides of the Atlantic, in the US and the UK. The new Security Strategy of the United States published in May 2010 defines cyber-threats as one of the most serious concerns the nation faces (The White House, 2010). The US has accordingly appointed a 'Cyber-Czar', putting considerable resources at his discretion. The UK launched its first cyber-security strategy in 2009 in response to the growing threat Britons were thought to be facing (UK Office of Cyber Security, 2009). One of the features singling out cyber-threats from all others is that physical obstacles, including traditional borders, are helpless against them: so it is natural to suppose that these threats will also affect a small country lying between these two great powers, namely Iceland.

## Iceland in a Changing Security Environment

Iceland's own security situation has changed significantly in the last few decades. In 2006 the US left the country after having maintained a military base at Keflavik for more than 50 years. The US rationale was that Iceland had lost its once high strategic importance, since modern warfare was now more and more taking place in a Middle East/West Asian 'arc of crisis' where assets pinned down in Iceland had no real relevance. While the US base was there to guarantee quick access by US troops, any threat Iceland faced under the old East-West military agenda might be considered fully covered by the US's deterrent power, with NATO as a whole behind it. Now that the US has left, Iceland has no special protected status, no troops of its own, and as will for instance be seen in the case of Estonia mentioned later, the universal mobility of cyber-enemies makes any country a possible target. The most relevant question is then, is Iceland really a potential target for cyber-criminals?

In fact, traditional military threats were never really the main issue for Iceland. The major ongoing threats the country has faced since independence were rather of the natural sort, and the volcanic eruptions in 2010 show that nothing has changed. Economic security problems have also been present, and still are in many respects. Active threats have been answered with military responses, as in the Cod Wars of the twentieth century, but the Icelandic mentality seems to find it hard to classify problems that do not present themselves in such physical and violent terms. (A general reluctance to think about 'security' needs may be related to the widespread popular aversion towards words like 'defence' and 'military'.) Traditional natural threats may be well understood and dealt with, no matter under what name, but the modern range of security concerns that any responsible nation needs to be alert to goes much wider than that. Britain's placement of an Icelandic bank on a terrorist regime list in 2008 gives one example of how aggressive behaviour can arise in spheres other than the purely military threat axis.

Another, and globally recognized, example of new violence is the terrorist threat that gained such prominence after 9/11. Large scale attacks no longer need a state sponsor to do massive damage, and non-military, civilian targets are often the first choice for terrorist aggression. Further, while traditional military confrontations still exist in the world, most cases of modern armed conflict are internal ones where the sides have changed from a military vs. military to a military vs. civilian or civilian vs. civilian contest; where any kinds of 'rules of war' are hard to enforce, and where it is not always clear who is winning. NATO itself has had to re-focus in the post-Cold War world to see if it can find a new place on the anti-terrorist and conflict-related battlefield: and experience in Afghanistan shows how tricky this new agenda can be even for such a powerful alliance.

Although Iceland may have passed somewhat out of the security loop in the last years with the Cold War's end and the departure of the US, that could in fact be changing in the coming years. The opening of the Arctic region could bring this territory back into the strategic spotlight and put new pressure on Iceland to determine where its priorities lie (Foreign Ministry of Iceland, 2009b). Many different questions arise under the new High North agenda, notably whether Iceland intends to claim some right to resources found there, but also what new security threats will affect Iceland as a result and how it intends to respond.

## A typology of cyber-threats

To see where cyber-threats come into this picture we must first specify what the threats are. They have been catagorized into three classes, all inter-connected (Cornish, Hughes, & Livingstone, 2009). The first category is probably the best-known personification of cyber-crimes, namely the lone hacker. While the image is often of the teenager with too much time on his hands, the hacker is actually more often a well-educated adult male. The reasons behind a particular cyber-crime can be very diverse, varying from the simple urge for vandalism to bragging rights or financial gains. While the damage the lone hacker can inflict may vary, he is seldom truly alone but rather one of a network of like-minded individuals. These people connect through forums and social networking sites where hacking tools are often offered to anyone interested. These sites can start trading in stolen account numbers and personal information that are often sold to the highest bidder: and while websites offering such services are often being taken down by law-enforcement officials around the world, there are always more available. Sites such as these are most often a part of the modus operandi of large international criminal organizations, who use them to handle stolen merchandise but also to recruit new hackers. These organized criminal organizations then form the second class of cyber-offenders (Cornish et al., 2009).

While the size of these organizations may vary, the largest of them have been seen to develop as a one-stop site for anything connected to cyber-crimes and illegal online-activity. That includes trafficking in personal and credit card information as already mentioned, but can also mean child pornography and manuals intended for terrorist cells and organizations. This can all be combined on a single site, hosted by the criminal group itself. Several organizations are offering 'bullet-proof hosting' for individuals or groups who want to build a site with illegal material. Bullet-proof hosting means that in the case of attention from law-enforcement officials the customer will be given ample time to save his illegal material before the site is closed, and the same site can then be opened at another location with little to no down-time.

The main threats posed by these organizations are often connected with Trojan viruses and spam. The sequence can be summarized thus: a member of the criminal groups writes a Trojan programme designed to infect computers and steal information from them. The infected computer is then used in order to infect even more computers, most often by using spam i.e. mass-sent e-mails preying on the curiosity and greed of the average computer user. These infected computers will then continue to try to infect more computers until the Trojan is eradicated from the system. Some Trojans even have some form of evolutionary potential, evolving to keep pace with the methods used to eradicate them. The network of infected computers, which may be counted in the millions and is commonly called a 'botnet', can then also be rented to interested parties - for instance to join in on an attack on any other site on the internet. One computer could be called a single soldier in this army of computers. A traditional cyber-attack involves this computer network all trying to access one computer or a small network of computers at the same time. While most sites are ready to handle a certain amount of computer traffic, if that level is exceeded the site will not be able to handle it and will most often be shut down. This is called taking a site off-line. Defences against a cyber-attack of this type would consist for instance of pre-limiting access by traffic from a certain computer or even region. This should keep traffic to a manageable level, but in a well-organized cyber-attack the attacks will be coming from such diverse areas that such simple methods will not be effective. These cyber-armies can be rented by groups or even individuals for an often modest fee, but the same methods are used by states that are actively attacking other states: blocking or distorting official sites, attempting to steal information, and planting cyber-mines.

The third category consists of cyber-threats directed at states and can be orchestrated both by other states but also by individuals and groups, with cooperation between these actors also being possible. Several states are already actively making cyber-weapons a part of their arsenal, but the extent of true cyber-attacks executed so far is not clear. The world today seems relatively free of military campaigns, but that does not mean that cyber-weapons are not being used even between 'friendly' nations. One possibility is for a state to enter another state's system and plant a cyber-mine in that system, for instance in the electrical system for a large city or even the whole country. In the case of a military conflict between these nations, the mines would be activated and the system either damaged or even taken off-line for some time. Such a major attack could be triggered through the telephone lines, without any soldier having to fire a single shot (Cornish et al., 2009).

An excellent example of all these manoeuvres was the cyber-attack on Estonia in 2007 (Traynor, 2007). The trigger for the attack is generally considered to be the planned move of a Soviet war-memorial statue that had for a long time caused discord in Estonia. On the morning of the projected move, the Estonian state came under cyber-siege. Estonia had been in the forefront of technological advances and relied heavily on computers and computer systems, which caused the attack to be even more severe. Although the attack took several sites off-line, for instance some newspapers and the site for the Estonian president, its real effectiveness can be disputed. The disrupted sites did not stay off-line for long and in the end the statue was indeed moved. The attack did, however, draw serious attention to cyber-attacks and - since Estonia was a member of NATO - also raised interesting questions about whether the alliance's common defence clause in Article 5 included joint reactions against cyber-aggression. In the end NATO established a Centre of Excellence in Estonia and has continued to raise the priority of cyber-threats as a serious and imminent threat.

The culprit for the cyber-attack on Estonia is still at large. Although Russia seems to be the clearest suspect, authorities in Moscow can claim plausible deniability and in the international arena that will suffice. Online evidence seems to indicate that there was a great online surge against Estonia on that particular date, with connections to Russian criminal organizations that were linked in their turn to Moscow. It has been argued that the strategic targets chosen in the attacks indicated state sponsorship, but the fact remains that while Russia denies having been behind the attack, nothing can be proven.

Another aspect of cyber-activity between states is cyber-espionage. This means a state employee trying to access a computer system of another state in pursuit of valuable information, for instance industrial secrets or other sensitive material. Although reported occurrences of cyber-espionage between states are not many, there is some evidence that incidents might be going un-reported. First, both states and institutions may feel there is a certain shame connected with being cyber-attacked. Such an attack means that someone has entered your private area without your being able to stop him, which could be seen as a sign of weakness. A company that has suffered a cyber-attack might hesitate to report the incident knowing that this might lead to fewer customers trusting the company. A state might also be reluctant to report that it was unable to defend its citizens. Secondly there is also the fact that cyber-attacks can be masked to conceal their origins. Thus when an attack or breach appears to come from a certain country or region, it might also be coming from somewhere completely different.

## Iceland's cyber-exposure

Iceland's position regarding cyber-use is somewhat peculiar. This country has long been proud to be in the forefront for many technological advances, and its population for instance ranks very high when it comes to the rate of use of computers and the Internet (Nordic Council of Ministers, 2009). Just this year, Iceland has claimed a leadership role in exploring another aspect of the freedom of the Internet by offering a home for electronic publishing by 'whistle-blowers', such as Wikileaks (Vallance, 2010). But that does not tell the entire story. True advances in technology are in fact twofold: the use of the technology, and the security that needs to accompany those advances. The latter is where Iceland is lacking (Jón Kristinn Ragnarsson, 2010).

One of the reasons Iceland has not considered security very important is the geographical location of the country. Being far from any other country makes Iceland relatively safe in traditional military terms, where soldiers need to travel over terrain and water to reach the opponent. But it is obvious that this cannot be the case with cyber-warfare. The soldiers of a cyber-army travel through the telephone lines and are not affected by traditional borders. While there might be people in Iceland who would propose to block even this by disconnecting the country from the outside world, that is hardly a practical scenario. And while Iceland is connected to the outside world, cyber-threats for Iceland are a viable possibility.

Iceland has been a partner in Nordic cooperation for many years, and a report reassessing that cooperation was commissioned from Thorvald Stoltenberg, a noted Norwegian politician, in 2009 (Stoltenberg, 2009). He was asked to offer suggestions on where Nordic security cooperation could be expanded beyond its present level. The report included 13 proposals that ranged from war crime investigation units to monitoring of Icelandic airspace, but also included setting up a Nordic resource network to protect against cyber-attacks. Since the release of the report this idea has already been pursued among the Nordic countries, with experts' meetings taking place including in Iceland. Those meetings, although just recently established, can be taken as showing that Iceland together with its neighbours takes the issue seriously, and that is certainly a good thing (Stefán Snorri Stefánsson, (PTA) e-mail communication, 2010).

However, the only real step that Iceland has taken lately towards systematically assessing its own security vulnerability was the appointment of an independent Risk Assessment team that presented its report in March 2009 (Foreign Ministry of Iceland, 2009a). 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. While the assessment found that cyber-threats did not have a high probability for Iceland, it identified them as one of the best options for anyone who might want to attack the country - precisely because they side-step the geographical factors obstructing a traditional military attack.

In fact, Iceland is lagging behind all other Nordic countries and most other relevant analogues in one specific regard, namely the establishment of a CSIRT team. (Computer Security Incident Response Team) In other countries this team would handle the cyber-defences of Icelandic civilian networks. Military networks are then handled by independent military CSIRT teams and other computer networks can have their own team, for instance in universities. Yet again the peculiarity of Iceland is seen in the fact that while it is a military-free country, no clear agent exists to handle the cyber-defences of the Iceland civilian sector either. The Icelandic Defence Agency, while operational, only handles the defences of its own network in accordance with its obligations towards NATO, while the civilian sector is unmanned. There has been some work done on options for setting up an Icelandic CSIRT team, in committees at the Ministry of Transport, but it has been bogged down for some time due to limited funding. This might reflect the general lack of security mentality in the Icelandic elite, but perhaps also the fact that the actual threat posed by cyber-attacks is still unclear in Iceland. As can for instance be seen with the recent vulnerability of the financial and economic sector - it seems that Iceland needs to fall victim to a threat before it will recognize the threat, but that state of affairs is clearly less than optimal.

## What next?

One good way to overcome this inertia is for Iceland to pursue practical, coordinated cyber-defence measures in the Nordic network where it feels most at home. However, the personal ties and the trade, transport, tourism and communication networks that bring cyber-vulnerability with them now link Iceland intimately not just with these near neighbours, but literally the whole world. For efficiency's sake also, it would be good for such a small state to 'pick the brains' of as many other partners and organizations as it can so as to arrive quickly and cheaply at a level of best practice. Here again we see the fundamental change of security conditions in the fact that working only, or mainly, with Iceland's earlier protectors - the USA and NATO - would not meet anything like these country's whole needs. NATO is a military institution that cannot control or make rules for economic and social actors, or claim to deal with civil crimes. The institutions that have most systematically focussed on solving today's cyber-threats start, in fact, with the Council of Europe which has published The Convention on Cybercrime, aiming to harmonize international efforts in this field (Council of Europe, 2001). Other relevant conventions aim at the internet service provider and security when it comes to cloud computing.[1] The EU has also

[1] Cloud computing involves a 'cloud' of computers hosting information for clients, instead of a single computer. Among the legal challenges is to determine to which jurisdiction the cloud belongs, and then what laws to abide by.

made attempts to harmonize legislation between member states, and to promote cooperation and consistency between international organizations that have interests in the matter. Because of the cross-border nature of cyber-crimes, universal standards for legislation and enforcement are the only sure way to eradicate 'safe-havens' and to ensure that some court, somewhere, is able to try any cyber-offender in future. As a full member of the Council of Europe and linked with the EU through the European Economic Area, Iceland can walk through an open door to tighten its cyber-cooperation both with these institutions and others.

These details point to a truth that applies much more widely to Iceland's security situation today. It can no longer rely simply on being protected either by its geographical situation, or by old allies who consider that situation important. Effective help, protection and partnership in technical advances is needed from a much wider range of states, neighbours and other Europeans and perhaps other like-minded nations further afield: and from a number of different institutions with varying competences and resources. If the options seem confusing and time-consuming, that does not mean that Iceland could not get a very good bargain for the country - in terms of the security won against the efforts spent - with a skillful policy based on cooperation between both official and non-state experts.

Indeed, here as in several other security-related fields, the moment when Iceland has found a good solution for its own needs is also the moment when it can start being a giver and helper for others. The world's poorest states are also liable to become cyber-victims as soon as their societies and national systems become dependent on any kind of cyber-technique, including the cyber-systems of their aid-givers. Just as it does already in the fields of fishing technology, geothermal power extraction, sustainable use of the environment and gender rights, could not Iceland aspire to become a model and helper for the world's less fortunate countries in the sphere of peaceful and efficient cyber-security as well? This would allow Iceland to play a part also in the universal spreading of best practice, rather than running the risk (by omission and ignorance) of offering safe channels to cyber-criminals - or chasing the illusion that cyber-safety can be built in isolation.

# References

Cornish, P., Hughes, R., & Livingstone, D. (2009). *CyberSpace and the National Security of the United Kingdom*. London: Chatham House. Retrieved August 3, 2010, from http://www.chathamhouse.org.uk/publications/papers/download//id/726/file/13679_r0309cyberspace.pdf

Council of Europe. (2001). *Convention on Cybercrime*. Budapest: Author. Retrieved August 9, 2010, from http://www.coe.int/t/dc/files/themes/ cybercrime/default-_en.asp

Foreign Ministry of Iceland. (2009a). *Áhættumatsskýrsla fyrir Ísland (Threat Assessment for Iceland)*. Reykjavík: Author. Retrieved August 5, 2010, from http://www.utanrikisraduneyti.is/media/Skyrslur/Skyrsla_um_ahattumat_fyrir_Island_a.pdf

Foreign Ministry of Iceland. (2009b). *Ísland á norðurslóðum*. Retrieved August 16, 2010, from http://www.utanrikisraduneyti.is/media/Skyrslur/Skyrslan_Island_a_nord-urslodumm.pdf

Jón Kristinn Ragnarsson. (2010) *Cyber-Security and Critical Infrastructure Protection: The Case of Iceland*. Unpublished MA thesis: The University of Iceland, Faculty of Political Science, International Relations.

NATO. (2010). *NATO 2020: Assured Security ; Dynamic Engagement*. Brussels: NATO. Retrieved August 7, 2010, from http://www.nato.int/strategic-concept/experts-report.pdf

Nordic Council of Ministers. (2009). *The Nordic countries in figures 2009*. Copenhagen: Author. Retrieved August 6, 2010, from http://www.norden.org/is/publikationer-/2009-748

Stoltenberg, T. (2009). *Nordic Cooperation on Foreign and Security Policy*. Oslo: Ministry of Foreign Affairs of Norway. Retrieved August 5, 2010, from http://www.utanriki-sraduneyti.is/media/Frettatilkynning/Stoltenberg_netutg_leidrett.pdf

The White House. (2010, May). *National Security Strategy 2010*. Retrieved March 1, 2010, from http://www.whitehouse.gov/sites/default/files/rss_viewer/national_-security_strategy.pdf

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Retrieved August 10, 2010, from http://www.guardian.co.uk/world-/2007/may/17/topstories3.russia

UK Office of Cyber Security. (2009). *Cyber Security Strategy of the United Kingdom: Safety, security and resilence in cyber space*. London, United Kingdom. Retrieved August 11, 2010, from http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf

Vallance, C. (2010, February 12). Wikileaks and Iceland MPs propose 'journalism haven'. *BBC*. Retrieved August 10, 2010, from http://news.bbc.co.uk/2/hi/850-4972.stm