STJÓRNMÁL & STJÓRNSÝSLA

Iceland and Cyber-threats:
Is it more than fear of fear?

Jón Kristinn Ragnarsson, specialist in cyber-threats
Alyson Bailes, Adjunct Professor at the University of Iceland

Abstract

The challenge of cyber-threats is a modern reality from which no state, including Iceland, can hope to escape. Cyber-attacks can cause major damage remotely, at minimal cost and while concealing the culprits. Groups and individuals can carry them out as effectively as states, reversing traditional power calculations and making deterrence especially difficult. Individuals can use the Net both for mischief and to escape from authoritarian controls; groups such as terrorists and criminals can target states, commerce and individuals; and states can attack other states both directly and by proxy. The complexity of possible online conflicts was seen clearly in the events triggered by Wikileaks disclosures against the USA in 2010 and 2011. Among other recent developments, an attack on the Pentagon and the 'Stuxnet' virus used against Iranian nuclear plants have shown how even the smallest devices can penetrate high-security systems, and that computer-driven infrastructures are no longer immune. Iceland, for its part, acknowledged the relevance of cyber-threats in its 2009 risk assessment, and recently decided to set up a coordinating team for protection; but it has lagged behind its Nordic neighbours in this field and should take full advantage of cooperation with them now. Vulnerable states also have an interest in international regulation and restraint on the use of cyber-weapons, but the context for this is complex and viable proposals are slow to emerge. Iceland can and should contribute to new thinking, and perhaps also assist poorer states: but it needs to put its own house in order first.

Útdráttur

Netógnir eru staðreynd sem allar þjóðir vorra tíma, og þar með taldir Íslendingar, þurfa að hafa áhyggjur af. Net-árásir geta valdið gífurlegum skaða úr fjarska, án greinilegs sökudólgs og án þess að miklu þurfi að kosta til. Hópar og einstaklingar eru jafnvíg ríkjum þegar kemur að slíkum árásum og setja þar með hugmyndir um valdajafnvægi á haus og gera vangaveltur um fælingarmátt

Stjórnmál & Stjórnsýsla 1. tbl.,7. árg. 2011 (187-204) Fræðigreinar

Vefbirting 30. júní 2011 – Birtist á vefnum http://www.stjornmalogstjornsysla.is
Útgefandi: Stofnun stjórnsýslufræða og stjórnmála, Gimli, Sæmundargötu 1, 101 Reykjavík

sérstaklega erfiðar. Einstaklingar geta notað Netið jafnt til illvirkja (eins og aðrir), en einnig til að sleppa undan ofurvaldi stjórnvalda: hryðjuverkahópar og glæpamenn geta ráðist á ríki, viðskiptaaðila og eintaklinga, og ríki geta ráðist á önnur ríki, beint eða óbeint. Það sást greinilega hversu flókin þessi mál geta verið þegar Wikileaks birti fjölda gagna um Bandaríkin árin 2010 og 2011. Þetta sýndu einnig hinar fjölmörgu árásir sem áttu sér stað á netinu í kjölfar þessara uppljóstrana. Aðrir nýlegir atburðir af þessu tagi eru meðal annars árás á Pentagon og 'Stuxnet' vírusinn sem miðaður er að írönskum kjarnorkuverum. Þessir atburðir sýna mögulegar flækjur og að mikilvægir innviðir eru langt frá að vera óhultur. Ísland hefur fyrir sitt leyti viðurkennd tilvist þessara miklu ógnar í Áhættumatsskýrslunni frá 2009, og hefur nýlega ákveðið að setja á stofn viðbragðsteymi til að samhæfa varnir gegn netógnum. Ísland hefur lengi staðið að baki öðrum Norðurlöndum þegar kemur að vörnum og ætti að nýta sér samvinnu með þeim á þessu sviði til fulls. Íslandingar geta og ættu að koma með nýjar hugmyndir til að hjálpa þeim sem ekki geta hjálpað sér sjálfir á þessu sviði Við þurfum þó fyrst að laga til í eigin garði.

Keywords: Cyber-threats, Iceland, Wikileaks, Infrastructure, Non-state actors

Introduction

Cyber-threats can justly be called the greatest new threats in today's world. This is true not only because of the scale of damage that cyber-attacks can cause throughout society, but also because the number of people who can be affected is not geographically or physically limited as in the case of attacks using other weapons. And since this is clearly a threat of the modern, globalized system, any state that wants to interact profitably with that system needs to take a policy stand on it, even if only to ask why the threat should concern it. In fact, unlike some other threats, cyber-threats constitute a category where inaction is not an option. While it is often possible for a small state to stay out of the forefront in security matters and to leave the toughest challenges to others, that does not necessarily work in the cyber-sphere.

It could be objected that no one has any possible motive to attack Iceland, whether with real or virtual weapons, and that defence generally is someone else's problem. The problem with this rationalization is that cyber-threats turn the normal realities of defence and security upside-down. Proof of identity of a cyber-attacker can often be very hard to establish, so that a hostile state can attack another state while concealing its role or even pointing to a different perpetrator. It is sometimes hard even to distinguish an 'attack' from a criminal scam or simple error (Bosch, 2004). The low cost and lack of accountability for cyber-attacks, plus a technology that makes it easy for individuals to inflict serious damage on states, mean that all normal calculations about possible motives for hostile action and about the disincentives against it are swept aside. Cyber-attacks could, for instance, be launched against an innocent state just for demonstration and trial purposes, or by a hacker

enjoying the technical challenge. In short, it is clear that every state aspiring to be a part of the international community needs to accept that cyber-threats are real and must be tackled, both in its own and in the general interest. The only question then remaining is whether the state wants to be a part of the international community. This is perhaps the first question that needs to be answered by policy-makers in Iceland.

Solving cyber-problems could in fact be an opportunity for a small state like Iceland – which itself threatens no-one - to take the lead, as some have already tried to do in the dimension of free speech (Hirsch, 2010). A suitable role for Icelanders would, for instance, be to help less advanced and poorer small states, which need not be a matter of expensive hardware but could be done through strategic know-how and technology transfer. However, it is necessary to learn before teaching. While important steps have been taken in the last few years, there is still far to go to protect Iceland's own cyber-security, as will be shown below. Further, threats are normally countered not just with defensive measures but with active attempts to outlaw and regulate unacceptable behavior: but in the cyber-realm this is proving exceptionally difficult, given the special circumstances and the complexity of the interests that need protection. This will be explained later in the article, where an assessment will be made of the prospects of reaching some kind of covenant between nations of the world on the use of cyber-weapons. Lastly, conclusions will be reviewed and the next steps for Iceland identified.

1 The theoretical context

Insofar as cyber-threats are used by one actor to seek advantage over another, taking advantage of a still largely anarchic virtual space, they can be addressed in the framework of realist international relations theory. But as the realist theory was developed some decades before the cyber-threat became a possibility, it needs to be expanded and adjusted to accommodate this new phenomenon. Cyber-threats have put massive weapons into the hands of the people, so that the principle in realist theory that the state is the most powerful actor becomes no longer necessarily true (Mingst, 2004; Nye, 2011). An individual can attack a state and inflict significant damage, in some cases even more damage than can a state. Again, the opposing parties do not have to be close to each other, or even on the same continent, for a cyber-attack to take place. The items used as cyber-weapons, most often meaning computer software and other similar devices, will from the outside look like any other computer system and can therefore be traded and taken across state borders without any difficulty. An entire arsenal can be kept on a flash memory drive that is no larger than a US cent. That leads us to the problem of deterrence.

In the Cold War era each side - the West and the East - had nuclear weapons. Each side knew that if it used its weapons, the other would respond in kind and both would be annihilated. This situation created a powerful deterrent that kept the Cold War relatively peaceful, except for some regional 'proxy' conflicts around the world.

Furthermore, in the case of nuclear weapons the warheads could be counted and their impact calculated, meaning that each side knew fairly well how many the other side had and how many would be needed to counter an attack. In the case of cyber-weapons this is impossible. Since there is no way for any state fully to know what the other state has in terms of cyber-weapons, it can really only assume the worst; and since the attacker has an excellent chance of concealing its identity, it has little reason to fear retaliation even from a well-armed victim. This situation seems bound to lead to an arms race of sorts, with states competing to master the most destructive applications of the technology while setting up the toughest defences against all comers. Many countries would of course prefer to stay out of such a race, believing they are not at risk: and Iceland has been of that persuasion for some time. In reality, however, as argued above, all states that rely on cyber-systems and are 'wired up' with the outside world are exposed by that very fact to substantial damage, both from attacks aimed at them directly and from the side-effects of cyber-attacks against their partners.

2 The cast and crew

As was seen in the previous section, cyber-threats significantly change the playing field of national and international security. Above all, they bring control and destructive power to the individual, and to various kinds of non-state groups, on an unprecedented scale. Even if states and groups of states can also gain new options for aggression, competition and self-defence by these means, in terms of relative gains all state actors have so far drawn the short straw. (Nye, 2011.) The new complexity of interaction in the cyber-world, and the leveling up of power status among different types of actors, may be considered for instance by looking at the course of the Wikileaks dispute of late 2010-early 2011.

This latest episode began when the whistle-blowing site Wikileaks released a new batch of documents disclosing communications between the US government and its embassies all over the world, including such embarrassing elements as descriptions of how foreign leaders were seen by the embassy staff and revelations of their unpublicized actions and opinions (Ellison, 2011). The Wikileaks movement was a small group of individuals clearly not acting on behalf of any state, but the US government nevertheless responded to the publication with the greatest seriousness, proclaiming that the actions of Wikileaks were a threat to American national security (Leonard, 2010). Among other things, this US reaction may be seen as an example of what has been called 'securitization' – that is, elevating an issue into the sphere of national security in order (usually) to justify harsh and exceptional measures in response (Wæver, 1995). One of the tests proposed by theorists for whether a successful act of securitization has occurred is whether the people at large accept that the matter has indeed reached the level of a public threat. In the case of Wikileaks, a certain number of people clearly did believe this and began to attack the Wikileaks site using cyber-weapons (Arthur, 2011). These individual attacks then provoked counter-measures by the other side, i.e. those who approved of the actions of

Wikileaks, and these pro-Wikileaks individuals (some belonging to another non-state group calling itself Anonymous) attacked online companies that had been persuaded by the USA to cease handling Wikileaks transactions . The resulting virtual battle lasted for several weeks, and can still not be said to have been fully resolved even several months after the release of the documents.

While this is only one small example, it is a good illustration both of the challenges posed by cyber-activity for traditional state power, and the complicated interplay of states, non-state groups and private citizens. Each of these types of actors will now be examined in more detail.

3.1 Individuals

In the traditional understanding of security, the isolated individual is relatively lacking in power and would certainly not be able to inflict any real damage on the state except in the rarest cases (such as top-level assassinations). With the introduction of cyber-threats, this has all changed. The individual can now, without much trouble, find or even make weapons that have the potential to disrupt the entire workings of many small to medium sized states. These tools can be found with a simple Google search, leading to instructions on how to manufacture cyber-weapons that can be used by anyone who pleases (Raywood, 2011). While there are not many examples thus far of individuals attacking states, there is plentiful evidence of individuals attacking other individuals, groups or smaller infrastructural facilities.

In the case of 'traditional' warfare and even of most non-state terrorist and sabotage attacks, knowing who is to blame has not been especially difficult, even though apprehending the suspect might be more troublesome. In the case of cyber-attacks, as noted, there are all too many options for the cyber-criminal to cover his or her tracks. Many open websites offer the option of routing the traffic through another country, so that the attack appears to be coming from somewhere else entirely. Options such as these have been used not only for criminal and destructive action but also for more positive, civil and democratic objectives. Many countries in the world have been trying to limit the use of the Internet by their citizens, and re-routing methods have helped the populations concerned and their supporters to exchange information and mobilize for action while avoiding detection by the oppressive state . This is a good example of how new cyber-technologies, and their impact on traditional power systems, can have two-sided, and often contradictory, implications for human security and welfare.

3.2 Organizations and groups

There are ample examples of groups using the Internet to their advantage, and there are also groups that have gone to 'the dark side' of the web. The Internet may be viewed as an extension of the traditional world in the sense that everything that can be found in the world can also be found on the Internet, and in that respect it comes as no surprise that terrorists, other extremists, and organized crime have taken to the Internet in a big way. The idea that fueled the building of the Internet to begin with

was a vision of diverse connections with relatively low overhead cost. This is, of course, ideal for terrorist cells such as Al Qaida. (Cornish, Hughes, & Livingstone, 2009) The world's best-known terrorist organization has taken to the Internet in a big way, using cyber-space to train recruits and attempt to appeal to new members. A good web presence is, in a sense, as important for Al Qaida as it is for any other organization in the modern world, be it of the criminal persuasion or not. The anonymity of the Internet is, of course, very helpful for terrorist organizations, but so is the fact that there is really no need for central leadership, discipline and hierarchy in order for an organization's message to be spread. A message of terror, like any other 'viral' online product, can gain a life of its own on the Internet as members and interested parties will continue to push it onward with no need for further effort by the originators. The Internet can, of course, also be used by anti-state actors around the globe to communicate and organize themselves in a virtual world without raising the attention of local or international law officials.

Criminal organizations are among those that have taken enthusiastically to the Internet, perhaps simply because there was a vacuum that needed to be filled in the virtual sphere, or because the potential earnings in proportion to cost and risk can be far greater than in most other versions of crime. One of the simplest versions of cyber-crime, which some would perhaps even hesitate to call a crime, is spam. All users of the Internet have at some point in their browsing history been spammed, and most have brushed it off as an insignificant nuisance. The truth is that spam is a huge industry, growing with each passing year. Several years ago, in 2007, Symantec – a world leading malware fighting company - detected 62,000 new infected computers each day (Cornish, Hughes, & Livingstone, 2009). These numbers are from four years ago, so it can be assumed that they have risen immensely, but 62,000 infected computers is still quite a high number. These infected computers come under the remote control of the maker of the malware, who can then either manipulate them directly or sell or lease the control to someone else. The infected computers, sometimes referred to as bots, will continue to try to infect more computers, attempting to increase the size of the maker's 'bot-net'.

One of the methods an infected computer will use to infect other computers is by sending out massive volumes of spam from the infected computer. The spammed letter and the list of recipients will always come from the controller of the bot-net. As was stated above, spam is a growing industry that can be explained in the simplest terms as targeted mail (mbl.is, 2011). To start with, once an e-mail address is known and has been verified as real, it can be sold for a very low amount, estimated as 1 US cent, to those intending to exploit it. If more information is known about the owner of the e-mail address, for instance the age of the owner and origin of the address, that address can be sold for a little more, estimated at 5 cents. This information can be gathered through various different sources, for instance by cross-referencing commercial and social networking sites with the known details. Lastly, the owner can be contacted to try to trick him/her into giving up the coveted information voluntarily. This attempt is most often called 'phishing', and can be carried out on a large scale to

try to gain either personal or financial information. It can be seen that the more information the sender of the phishing attempt knows about the recipient, the more likely it becomes that the latter will give up more information. To put it simply, if someone approaches you and is already in possession of information that only trusted contacts should have, the more likely you are to entrust them with more.

3.3 States

When it comes to states being attacked by cyber-weapons, the evidence is less plentiful – for a curious reason: there seems to be a certain shame connected with being infiltrated by cyber-attacks, on the argument that if a state cannot defend itself against such phantom enemies, how can its citizens trust it to protect them more generally? Although this attitude is of doubtful logic – not least because states can best foil attacks when citizens are alert and actively help them - it goes a long way towards accounting for the fact that not as many attacks are reported as must surely have occurred in reality. Some cases of almost certainly state-originated cyber-attacks have received the publicity they deserve, such as those involving Estonia and Georgia , but there are also incidents that have gone mostly unnoticed, such as the attack on the Pentagon in 2008 (Mills, 2009) and the 4th of July attacks of 2009 on the US and South Korea (BBC News Technology, 2011). Perhaps the level of publicity is determined by the results rather than the intention of the attacker, for reasons that will be further discussed below.

The attack on the Pentagon is noteworthy in many respects, and has been called one of the greatest attacks ever carried out against US defence assets. It also underlines the fact that the most successful attacks do not always have to involve heavy weaponry. It was launched with a single flash-memory drive, left at an open location by an unknown agent for a Pentagon employee to find. That employee took the memory drive to his work computer and plugged it in. As the memory drive was loaded with malware designed to infect any computer it came in contact with, and as the Pentagon network is close-knit, a great number of computers became infected as a result. A couple of further lessons from this event are worth noting. The first is that following the attack, the Pentagon banned the use of any flash memory drives in its computers: an example of a cheap and simple defence measure, taken belatedly only after the threat had been directly experienced. Secondly, the extent of the damage from so small a cause underlines that the technological advances involved are sometimes staggering.

The Stuxnet virus discovered in the summer of 2010 at an Iranian nuclear power plant is another cyber-threat that has changed the entire international spectrum as more and more information has subsequently been revealed about it (Gross, 2011) It was clear from the outset that the virus seemed to target a very specific type of computer, namely computers that were integrated into the production and operating processes of certain industrial plants. Not only could the virus disrupt these computers; it could also send information from the infected systems back to the maker of the virus. These were both factors that were quite new in the field of cyber-threats, and

yet more were to be reported. It has been widely assumed that the virus was made by the USA and/or Israel in an attempt specifically to disrupt Iran's nuclear activities (Broad, Markoff, & Sanger, 2011), as Stuxnet appears too sophisticated for an individual or small group to create without at least the aid of a state. The cyber-systems controlling critical infrastructure, in the power industry and elsewhere, are most often disconnected from the greater Internet as a defence mechanism, making it more difficult for any malware to reach these important computers. The success of Stuxnet suggests that the makers of this malware were not only very well informed but a step ahead of the defensive side of the game. While Siemens, the makers of the relevant control systems, rushed to close off the specific vulnerabilities that were revealed (Marks, 2011), it is widely agreed by experts that Stuxnet has changed the whole landscape of international relations – for better or worse – and drawn the attention of policy makers to cyber-threats more emphatically than ever before (Mills, 2010).

Yet another significant aspect of the cyber-threat against states is its application to espionage. It can be assumed that states hold many secrets within their computer systems, where they are accessible to anyone who can infiltrate those systems. At the same time, because of the feelings of shame that were mentioned earlier, no state is likely to admit freely that its systems have been breached. Thus a free market of sorts has developed where states and individuals can work to infiltrate the systems of other states and large companies without there being much recourse against them. Thankfully, it has been concluded that there is no industrial espionage going on in Iceland (Halldórsson, 2010). Yet even though the Minister of the Interior has expressed doubt about any espionage taking place in Iceland, it seems he has realized that Iceland is still a part of the outside world, as the next section will reveal.

4 What is the situation in Iceland?

For a very long time, defence was hardly present on the Icelandic national agenda and, as the joke went, all such matters were outsourced to the USA. Then in 2006, when Washington decided unilaterally to withdraw its forces from Iceland, the country suddenly had to face the prospect of handling its own security. In the five years since the departure of the US army, Iceland has certainly made steps in that direction, but they are baby steps at best. The first logical stage was to determine what the risks for Iceland today may be, and cyber-threats duly appeared among those mentioned in an independent risk assessment report delivered in early 2009 (Foreign Ministry of Iceland, 2009). This report assessed cyber-attacks against the Icelandic state as not very likely, but it should be noted that most of its analysis was completed in 2008, before the Icelandic economic collapse and everything that it led to. There is good reason to assume that the situation may have changed in the meantime. Even so, the 2009 report thought it worth proposing that Iceland establish a response team (ICE-CSIRT – Computer Security Incident Response Team) of the same type as is found in its neighboring countries, including the other Nordic states. The Icelandic state

took some time to reflect on this before finally authorizing the establishing of a response team, under the authority of the Post and Telecommunications Authority (PTA), in October 2010 (Jónasson, 2010).

The tasks such a team must handle are of many types, and its success will depend on several key features. The team should provide all actors in the Icelandic system with information about the present threats and guide them in taking protective measures, as well as establishing cooperation with various agents in relevant institutions and partner states abroad (see below). Within Iceland, the authorities responsible for management of all key infrastructures and services, including the government's own online operations, will need to collaborate; this collaboration will have to include some private agents such as internet service providers and telephone companies. For a team to be able to bring together all these agents and to gain their cooperation and trust is no small matter, and the placement of the team within the government could be a sensitive point. There is reason to fear that placing this important team within a long-standing sectoral agency, which has for the most part acted as a disciplinarian over the actors it now needs to unite, could also too easily doom it to fall short in its goals. Time will tell how the team will survive, but the starting position can be considered far from ideal.

There are certainly other resources in Icelandic governance that might give hope regarding the protection of the Icelandic people in this crucial dimension. The now defunct Defence Agency would have been a good place to address, especially, the more strategic aspects of the country's cyber-defences, but it did not survive to see that happen. The office of the National Police Commissioner, with its broad responsibilities for civil protection, would also be a likely place, and that department of the recently enlarged Ministry of the Interior has been coming up with some interesting initiatives in recent months. The latest of these would involve the authorizing of pro-active measures aimed at organized crime, which has begun to take root in Iceland (mbl.is, 2011). As was mentioned in Section 3, there are certainly connections between crime in the virtual world and in the real, and the kind of organized crime that is starting to spread in Iceland is no exception. The most important signal sent by such moves, however, is that although Iceland is an island, it is still a part of the greater world and must recognize that all and any of today's typical transnational threats can also present themselves in the country.

This reality also has an important positive side: namely, that Iceland is far from alone in facing the cyber-challenge. Its security in this sphere is also an important link in the chain for its neighbours and its NATO and EEA partners, and it has correspondingly full access to the cooperative frameworks involved. As so often, the other Nordic states are the natural first place to look for close cooperation; and they have in fact developed some important skills, both public and private, in supplying cyber-security for societies organized along similar lines and values to Iceland's. In 2009 when reporting to the Nordic Council of Ministers on room for improvement in Nordic defence and security cooperation, Thorvald Stoltenberg included cyber-affairs as a high-priority aspect of civilian security. (Stoltenberg, 2009) In a declaration

of 5 April 2011 that included a general statement of 'solidarity' against non-traditional threats, the Nordic Foreign Ministers duly confirmed their readiness to cooperate on cyber-defences as a kind of model for other fields. (Foreign Ministry of Iceland, 2011). It is interesting to note that they mentioned cyber-threats in the same sentence as terrorist attacks and large-scale natural disasters – revealing that the Nordic countries treat cyber-threats as seriously as do other European states, or even more so, by elevating cyber-security to the highest category of possible threats. These developments are all very much in Iceland's interest, and they show that Iceland has been far from lacking in influence over the whole handling of the Stoltenberg exercise. It cannot expect, however, to gain full value from such cooperation unless it can offer the appropriate tools and contact points, including above all a really effective CSIRT.

5 Beyond defence: The debate on global regulation

For any state that is vulnerable to cyber-threats, and especially one that has little defensive power of its own, the idea of action to limit and reduce the threats at origin must be very attractive. The logic is just the same as for the control and reduction of traditional armaments, a cause that Iceland has always strongly supported. However, international efforts to govern, and particularly to regulate, the realm of cyber-security are fraught with several kinds of difficulty. First, the world's democratic powers have hailed the Internet as a basically positive tool of communication, openness and empowerment that has played a role in liberation and reform processes – as seen most recently in the Arab world – as well as allowing the whistle to be blown on abuses within the West. Such political views, coupled with business interests, have militated against consensus on any strict global scheme of regulation during previous UN meetings held to discuss the new media. The most notorious attempts to control access to the Net and block sources of unwelcome information have been made by individual states like China, and have been strongly criticized by the USA in particular: thus Secretary of State Hillary Clinton felt it necessary to stress the general principle of cyber-freedom even at a moment when - in February 2011 - the USA itself was bringing injunctions against Wikileaks collaborators (World News, 2011).

The challenge of security-related IT regulation thus presents itself as a typical 'dual-use' one, similar to those faced by the nuclear, chemical and bio-industries whose work is overwhelmingly legitimate and even benign, but where 'firewalls' are needed against the destructive use of related materials and techniques. The logical conclusion would be that security controls on online activity need to be minimal, transparent and sensitively adjusted to avoid 'collateral damage' to innocent service providers and users. Further, it must be recognized that there are actually multiple rationales for protective regulation – state security-related, law and order-related, commercial and intellectual property-related, human rights-related (privacy), and ethical (as with banning pornography). Even if each aspect is promoted by different groups for different reasons, pursuing them too much in isolation from each other could risk confusion, waste of effort and probably an over-restrictive outcome.

The second side of the problem is that the threats and abuses needing to be addressed are equally diverse - as everything in this article so far has shown – and it is almost impossible to find ways of attacking through the Net that can only hurt 'bad' actors without the risk of being turned back against 'good' ones. Cyber-crime, the most fully and widely developed cyber-threat, is surely everyone's enemy, as is the unmotivated and irresponsible solitary hacker. All states should wish to stop the use of new media to run terrorist networks, to spread knowledge of how to make Weapons of Mass Destruction and other lethal techniques, or to distribute child pornography. Beyond this, however, come techniques that states – as well as non-state movements – may wish to exploit against each other, ranging from information blockage, invasion of official websites and service denial through to the direct sabotage of infrastructures and/or defence assets, as in the 'Stuxnet' case already discussed (Gross, 2011). Designing suitable controls against these is doubly difficult since the same technical knowledge is often required for defensive as for offensive measures; thus, few states are likely to be willing to give up the relevant capacities even if they would be ready to outlaw certain actions. Finally there are legal net-based activities that states may be happy to see used against their opponents but not against themselves, like the stirring up of protest movements, planning of potentially violent demonstrations and publicizing of inflammatory secrets.

A further set of difficulties arises from the fact that the phenomenon of Internet and new media use is overwhelmingly driven by non-state actors such as businesses, social movements, NGOs and individuals. The scope for dangerous actors of this kind to damage states, and indeed for states to manipulate them and hide behind them, has already been demonstrated above. On the other hand, private firms and consultancies provide some of the most technically advanced and energetic defences against cyber-attacks of all kinds. The problem of discouraging and punishing the 'bad' and mobilizing the 'good' efforts of private actors is of course hardly new: it arises in just about every field of modern security, from anti-terrorist and anti-WMD strategies to combating climate change (Bailes, 2007). Military power is rarely, if ever, the answer and even direct physical interdiction is difficult, as is shown, for example, by the small number of cyber-offenders who have ever been caught and brought to justice. The alternatives that remain may be empirically categorized (Bailes, 2007) as:

legally outlawing certain activities by non-state actors and requiring both states and non-state parties to help enforce the ban;

laying down safety and security regulations for the conduct of other online activities that are permitted in themselves but should be guarded against abuse;

directly influencing the behaviour of businesses and other non-state groups, e.g by fiscal carrots and sticks and by state favours to those who can prove their law-abiding nature;

encouraging self-regulation and self-restraint by all kinds of users, such as codes of conduct for businesses, scientists and media organizations, computer safety practices for individuals, public help with threat alerts and investigations, etc. and

encouraging legitimate businesses and organizations, in the same way as state

entities, to take passive and defensive measures to 'harden' vital computer-driven systems, prepare fall-back systems, practise emergency protocols and so forth.

Another useful way of conceptualizing security measures for non-state actors is the system proposed by Professor John Ruggie to the UN Human Rights Commission for reducing business offences against human rights (Business & Human Rights Resource Centre, 2011). He identifies the three following phases: i) 'Protect' by national and international regulation, ii) 'Respect' through business compliance and self-regulation, and iii) 'Remedy' by ensuring that every kind of abuse has some legal mechanism for hearing complaints and bringing cases to trial. This last point is also highly relevant to the case of cyber-attacks, which can damage businesses and individuals as well as the interests of states and multinational institutions, but for which no specially dedicated court structure exists at present.

6 Some international initiatives

On the face of it, all the approaches mentioned above are worth exploring to find cooperative, non-violent solutions for cyber-security problems. The special challenges posed by the anonymity of many cyber-attacks and the use of non-state proxies may in principle be tackled by setting standards and finding remedies that are – so far as possible – equally tough on state and non-state offenders, and applying them with the widest possible state and non-state cooperation. What has the international community actually been doing to this end, and are there any particular lines of action that Iceland could and should support? It must be said that responses so far have been quite slow and confused, despite the length of time that some phenomena like spam and cyber-crime have been with us already. The bad news here is that there is a lot of ground to be made up, but the good news is that the field is still open for well-intentioned states and individuals to come forward with helpful ideas.

The strongest single international-legal measure so far drafted is the Council of Europe's Convention on Cyber-Crime (Council of Europe, 2001), which came into force in 2004 – and of which Iceland is also a signatory. Several other international organizations, from the United Nations downwards, have encouraged as many states as possible to sign this document, which also provides a solid base for inter-governmental police cooperation through Interpol and Europol. Its limitation is of course that it only addresses actions defined as crimes, rather than – for example – establishing the equivalent of 'laws of war' between states, or addressing issues in the ethical, human rights, and governance fields. Some have also criticized it for being based on inadequate consultation with the private sector, although it does encourage cooperation between state agencies and private service providers. However, it is noteworthy that no other major institution has yet come forward with an alternative blueprint for comprehensive global regulation. The UN has limited itself largely to general policy recommendations, the EU has focused on cooperation in risk assessment and protective measures, while NATO's programme – updated in its new Strategic Concept (NATO, 2010) – is centred on the defence of key military assets. There has

been no serious discussion within NATO of whether a cyber-attack on a member would require collective military action for defence and retaliation, and the Estonian events of 2007 were certainly not handled in that style.

The tit-for-tat attacks triggered by recent Wikileaks disclosures and the revelations about Stuxnet, as discussed above, have however brought new urgency to the international debate about the disciplining of cyber-space. At the annual security conference held at Munich in February 2011, the British Foreign Secretary, William Hague, complained that much of the work done by international organizations so far had been 'fragmented, and lacks focus'. He went on to call for 'a more comprehensive, structured dialogue to begin to build consensus among like-minded countries and to lay the basis for agreement on a set of standards on how countries should act in cyberspace' (Hague, 2011). President Nicolas Sarkozy of France carried the issue to a higher level by placing it on the agenda of the group of eight industrialized nations (G8) Summit at Deauville on 26-27 May 2011, where a lengthy political declaration was adopted calling for international solutions on Internet governance to protect 'personal data, net neutrality, transborder data flow, ICT security, and intellectual property' (G8, 2011). Western leaders taking such initiatives have, of course, been thinking primarily of their own security interests, and it is this state-centric focus that has also dominated preliminary discussions about regional cooperation against cyber-threats in other bodies such as the Shanghai Cooperation Organization, the Organization of American States, and the Asia-Pacific Economic Cooperation Forum.

Such state-led moves have in turn drawn criticism and warnings, most publicly, but not only, from the net operators themselves who fear creeping encroachment on both their freedoms and their profits. The US Atlantic Council, which has reflected on the issue for some while, has argued that non-state and economic perspectives need to be given due weight and that other norms, such as the protection of individual privacy, need to be built into any comprehensive system. An interesting attempt to approach the challenge from a more bottom-up, humanitarian perspective was made by a group of US and Russian experts convened by the New York-based East-West Institute (EWI), who raised the question whether an analogue to the Geneva Convention (which establishes 'laws of war' and of conflict to protect non-combatants, the wounded and prisoners of war) was now needed for the cyber-domain. The notion of 'war' would have to be redefined to take account of the virtual nature of cyber-activity and the wide range of participants, but the basic idea would be the same: namely to protect zones and facilities that are important for human welfare and for the survival of the innocent, such as medical facilities or transport safety systems. Complete bans on certain cyber-techniques could also be considered, on the analogy of the international laws that prohibit the most inhumane and indiscriminate conventional weapons, and the global restrictions on WMD.

Other ideas promoted by EWI include the possibility of a world court for the impartial judging of international cyber-offences and a stronger mechanism for dialogue with non-state actors. The Institute believes, however, that the protection of specific security interests is best approached for the moment at regional level, given

the diversity of threat patterns and variation in the common interests that need to be protected. This reflects the reality so far and is probably sensible. Differentiated local approaches make it even more desirable, however, to set some global framework for the larger questions of ethics, rights (including property rights), and human welfare that are at stake: and here – as already noted – the world community is open and even eager for new ideas. While playing its part in Nordic regional cooperation, Iceland would do well to reflect on what its experts in cyber-systems, law, ethics and security, both from the public and the private sector, could most usefully bring to this global level of debate.

7 Conclusions

Iceland has for a long time followed the 'see no evil' philosophy, meaning that if the threat cannot be seen it cannot be there. Luckily, in recent years this has begun to change. Yet Iceland as a state still has quite a way to go to get its cyber-security policies and actions on a par with those of its neighboring states; and while the establishment of a CSIRT team is a vital step it leaves much more to be done. Iceland has in recent years pressed actively for Nordic security cooperation in general to be improved, as reflected in the story of the Stoltenberg report mentioned above. Now that all five Nordic Ministers have agreed on cyber-defence as an area where they should aim for the highest solidarity and unity of action (Section 4 above), the onus is on Reykjavik to start taking fuller advantage both of this specific project and other still unexplored Nordic resources (Ragnarsson, 2010; Ragnarsson and Bailes, 2010). Once Iceland can claim to have caught up with the general Nordic standard of analysis and readiness in this field, then and only then will it be well placed to use its experience as a basis for raising awareness about cyber-problems among other states, and to offer assistance to those less well equipped. The important thing to note is that this step cannot be taken now, or later this year. The Icelandic mentality has often been to aim at being the best in the world from the word 'go', but people may now be starting to realize that such thinking has not necessarily brought Iceland very far.

The problem is not so much that Iceland lacks skills and ideas, but that pushing forward on one point – for instance, seeking maximum protection for leaks and whistle-blowers, rushing to exploit every new technical innovation, or relying even more on 'e-governance' for conducting public business – may do more harm than good when the general context and the balance of risks and benefits are not fully grasped. Among other things, anything that raises a state's profile of cyber-activism beyond the normal could in itself create critics as well as friends, and lead to attacks for which it may not be fully prepared. As a matter of more general principle, however, all human freedom - even online - needs a sense of responsibility: and responsibility should include protecting clients, the broader public, and legitimate state interests, as well as one's own operations, against the threats of both attack and abuse. As a small state with limited defence experience and defensive capability,

Iceland in practice needs help to reach acceptable standards in these areas. It would gain rather than lose credibility by acknowledging that fact. It might gain even more by entering the international debate with good ideas on the protection and regulation, as well as liberalization, of cyber-space.

Endnotes

1 Such attacks have, for example, recently been placed among the top five threats worldwide in NATO's new Strategic Concept (NATO, 2010) and in the UK's national defence review of October 2010 (The Independent, 2010).

2 This includes companies such as Paypal and Amazon, which declared they could not provide service to a website that was responsible for putting American soldiers at risk. (Arthur, 2011)

3 A good example can be seen in the recent democratic revolution in Tunisia (Los Angeles Times, 2011).

4 A bot-net is defined as a group of infected computers, perhaps hundreds or thousands strong, brought under the control of a another agent. It is a versatile tool that has also played a part in hostile state attacks, aiming for example to swamp and shut down a target site.

5 For more on the cyber-attack on Estonia in 2007 see Traynor, 2007, and on cyber-attacks during the war between Russia and Georgia in 2008 see Espiner, 2008. It is noteworthy that Russia was the suspect, and similar methods were used, in both cases. The attack on Estonia finally resulted in the establishing of a NATO Centre of Excellence for cyber-security based in Tallinn, and in a general raising of priority for cyber-threats within NATO's strategy (NATO, 2010).

6 For more on links between cyber-security and critical infrastructure in general, see Westrin, 2001 and Wenger, Mauer and Dunn (eds.), 2009.

7 The thousands of English and Dutch individuals who lost their savings in the Icesave accounts can be assumed not to be fans of Iceland, and as is mentioned in Section 3, cyber-threats can be used by individuals with little effort or cost. This is one of the reasons to assume that the risk has been elevated since the publication of the Threat Assessment.

8 The term CSIRT has for the most part replaced CERT - Computer Emergency Response Team - but CERT does still appear in related documents.

9 The Post- and Telecommunciations Authority could of course end up being the best possible place for a team such as this, but early indications are not encouraging.

10 See also Section 7 below

11 The non-military 'solidarity' clause in Article 222 of the European Union's Lisbon Treaty (European Union, 2009), to which three Nordic states are parties, highlights only terrorist attacks and large natural disasters as examples of events that should trigger maximum mutual aid and efforts aimed at prevention.

12 The US court actions in question were aimed at enforcing disclosure of mobile phone exchanges between individuals thought to have been involved in discussions about the mass transfer of State Department telegrams to Wikileaks.

13 A well-known case already mentioned is the use of the Net by Russian interests to stir up violent anti-government actions in Estonia. Evgeny Morozov (2010) has argued that oppressive regimes will eventually steal all relevant techniques from their opponents and use them to spread hate and slander campaigns, organize pro-regime counter-demonstrations and so on.

14 For details of the institutional measures mentioned in this paragraph, see Ragnarsson, 2010.

15 For a recent example, see European Union, 2011.

16 See Atlantic Council, 2011 for the latest activities of this organization.

17 The EastWest Institute is an independent not-for-profit 'think and action tank', with centres in both New York and Europe, that has made its name by holding East-West bridge-building meetings ever since the 1970s. The expert report in question was launched at the EWI's second international 'Cyber-summit' in January 2011, see EWI, 2011.

18 Provisions against inhumane weapons are contained in the 'Certain Conventional Weapons' (CCW) Convention of 1980, while the possession and use of WMD is regulated principally by the Non-Proliferation

Treaty, Chemical Weapons Convention and Biological Weapons and Toxins Convention.

Bibliography

Arthur, C. (2011, January 8). "Wikileaks under attack: the definitive timeline", The Guardian online, January 8 2011, Retrieved April 6, 2011, at

http://www.guardian.co.uk/media/2010/dec/07/wikileaks-under-attack-definitive-timeline

Atlantic Counil of the United States (2011). "International engagement in cyber: Establishing international norms for improved cyber security", 29 March 2011. Retrieved 21 June 2011 at http://www.acus.org/event/international-engagement-cyber-establishing-international-norms-improved-cyber-security

Bailes, A. J. K. (2007). "A 'New Deal' between State and Market", in Ø. Østerud & J.H. Matláry, Denationalization of Defence: Convergence and Diversity. London: Ashgate.

BBC News Technology. (2011, March 4)." South Korea hit by cyber attacks". Retrieved April 5, 2011, from BBC News: http://www.bbc.co.uk/news/technology-12646052

Bosch, O. (2004). "Defending against cyber terrorism: protecting the legitimate economy",in Bailes, A.J.K., Herolf, G., and Sundelius, B., Business and Security: Public-Private Relationships in a New Security Environment. Oxford University Press: Oxford

Broad, W. J., Markoff, J., & Sanger, D. (2011, January 15). "Israeli Test on Worm Called Crucial in Iran Nuclear Delay". Retrieved April 7 2011 from The New York Times - Middle East at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1

Business and Human Rights Resource Centre (2011). Wepbage of the UN Special Representative. Accessed 21 June 2011 at http://www.business-humanrights.org/SpecialRepPortal/Home

Cornish, P., Hughes, R., & Livingstone, D. (2009). "CyberSpace and the National Security of the United Kingdom". London: Chatham House.

Council of Europe (2001). "Convention on Cybercrime". Budapest: The Council of Europe. Retrieved 15 April 2011 at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

EastWest Institute (2011). "Report on the second Cyber-Summit, January 2011." Retrieved 21 June 2011 at http://www.cybersummit2011.com/component/content/article/26.

Ellison, S. (2011, February 1). "The Man Who Spilled The Secrets". Retrieved April 13, 2011 from Vanity Fair Politics:

http://www.vanityfair.com/politics/features/2011/02/the-guardian-201102

Espiner, T. (2008). "Georgia accuses Russia of coordinated cyberattack", Retrieved 21 June 2011 at http://news.cnet.com/8301-10093-10014150-83.htm

European Union (2009). "Treaty of Lisbon," entered into force 1 December 2009.

Retrieved 15 April 2011 from http://europa.eu/lisbon_treaty/full_text/index_en.htm.

European Union (2011)." Cyber Security: EU prepares to set up Cyber Emergency Response Team", 'Europa' portal 10 June 2011. Retrieved 21 June 2011 at

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/694&format=HTML&aged=0&language=EN&guiLanguage=en

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

Foreign Ministry of Iceland. (4. April 2011)." Samstöðuyfirlýsing utanríkisráðherra Norðurlandanna og málefni Líbíu" (Joint statement of the Nordic Ministers and the issue of Libya). Retrieved 12

April 2011 from Foreign Ministry of Iceland: http://www.utanrikisraduneyti.is/frettir/nr/6245

G8, Summit Declaration of May 26-7 2011 on "Renewed Commitment for Freedom and Democracy", Annex on "The Internet"', retrieved 15 June 2011 from http://www.g20-g8.com/g8-g20/g8/english/the-2011-summit/declarations-and-reports/declarations/renewed-commitment-for-freedom-and-democracy.1314.html

Gross, M. J. (2011). "A Declaration of Cyber-War". Retrieved April 1, 2011, from Vanity Fair online: http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

Hague, W. (2011). "Address to the Munich Security Conference", February 2011.

Retrieved 15 April 2011 at http://www.securityconference.de/Hague-William.622.0.html?&L=1

Halldórsson, J. H. (2010). "Efast um að Íslendingum standi ógn af iðnnjósnum" (Doubtful whether Iceland faces threat from industrial spies), 6 December 2010. Retrieved April 8, 2011, from Vísir.is:

http://www.visir.is/efast-um-ad-islendingum-standi-ogn-af-idnnjosnum-/article/2010344978629

Hirsch, Afua. (2010). "Iceland aims to become a legal safe haven for journalists", The Guardian online, 12 July 2011. Retrieved 15 April 2011 from

http://www.guardian.co.uk/media/2010/jul/12/iceland-legal-haven-journalists-immi

The Independent (2010, October 19). Sengupta, K. et al, Threat of cyber attacks the new priority as cuts hit major projects, retrieved 15 April 2011 from

http://www.independent.co.uk/news/uk/home-news/cyber-warfare-terrorism-and-floods-are-the-greatest-threats-to-britain-2110273.html.

Jónasson, B. (2010). "Stjórnvöld bregðast við hættu á netinu" (Government wrestling with threats on the net), 10 October 2010. Retrieved April 3, 2011, from Vísir.is:

http://www.visir.is/article/2010612178936

Los Angeles Times online (2011). "Tunisia protesters use Facebook", 14 January 2011. Retrieved June 21 2011 at http://latimesblogs.latimes.com/technology/2011/01/tunisia-students-using-facebook-and-twitter-to-organize.html

Leonard, T. (2010). "Pentagon deems Wikileaks a national security threat", The Telegraph 18 March 2010. Retrieved April 10, 2011, from

http://www.telegraph.co.uk/technology/7475050/Pentagon-deems-Wikileaks-a-national-security-threat.html

Marks, P. (2011). "Stuxnet analysis finds more holes in critical software". New Scientist magazine, 25 March 2011, London

mbl.is. (2011). "Senda um 300 milljarða tölvupósta á dag "(Sending around 300 billion mails a day), 13 January 2011. Retrieved April 8, 2011, from mbl.is:

http://www.mbl.is/frettir/forsida/2011/01/13/senda_um_300_milljarda_tolvuposta_a_dag/

mbl.is. (2011). "Rannsóknarheimildir lögreglu verða auknar" (Police's resources for investigation increased), 2 March 2011. Retrieved April 4, 2011, from mbl.is:

http://www.mbl.is/frettir/innlent/2011/03/02/rannsoknarheimildir_logreglu_verdi_auknar/

Mills, E. (2009, April 7). "Pentagon spends over $100 million on cyberattack cleanup". Retrieved April 10, 2011, from cnet news – Security, at: http://news.cnet.com/8301-1009_3-10214416-83.html

Mills, E. (2010, December 8). "EU Calls Stuxnet 'paradigm shift' as US responds more mildly". Retrieved April 5, 2011, from cnet news, at: http://news.cnet.com/8301-27080_3-20019124-245.html

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

Morozov, E. (2010). "The Net Delusion: how not to liberate the world". London: Allen Lane

North Atlantic Treaty Organization (2010)." Active Engagement, Modern Defence", NATO's new Strategic Concept adopted 19 November 2010, retrieved 14 April 2011 from http://www.nato.int/strategic-concept/index.html.

Nye, Joseph S. (2011). "The Future of Power", Jackson, USA: PublicAffairs.

Ragnarsson, Jón Kristinn. (2010) "Cyber-Security and Critical Infrastructure Protection: The Case of Iceland". M.A. Thesis in International Relations at the University of Iceland. Retrieved at URL: http://hdl.handle.net/1946/4781

Ragnarsson, Jón Kristinn and Bailes, Alyson. (2010)" Iceland and cyber-threats" in Þjóðarspegillinn, University of Iceland: http://hdl.handle.net/1946/6816

Raywood, D. (2011, April 11). "The denial-of-service ransom threat". Retrieved April 14, 2011, from Security Business Intelligence Magazine: http://www.scmagazineuk.com/the-denial-of-service-ransom-threat/article/200410/

Sengupta, K et al (2010). "Threat of cyber attacks the new priority as cuts hit major projects", The Independent online 19 October 2010. Retrieved 15 April 2011 from http://www.independent.co.uk/news/uk/home-news/cyber-warfare-terrorism-and-floods-are-the-greatest-threats-to-britain-2110273.html.

Stoltenberg, T. (2009). "Nordic Cooperation on Foreign and Security Policy". Oslo:

Ministry of Foreign Affairs of Norway

Traynor, I. (2007). "Russia accused of unleashing war to disable Estonia", The Guardian online, 17 May 2007. Retrieved 21 June 2011 at http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

Wenger, A., Mauer, V. and Dunn, M.(eds.) (2009). "CIIP Handbook 2008/9". Centre for Security Studies: Zurich

Westrin, P (2001). "Critical Information Infratsructure Protection (CIIP)". ProCon Ltd: Sofia

World News. (2. February 2011)."Clinton to lay out U.S. Internet freedom plan". Retrieved 7 April 2011 from World News: http://article.wn.com/view/2011/02/15/Clinton_to_lay_out_US_Internet_freedom_plan_e/

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