Clingendael
Netherlands Institute of International Relations

Policy Brief

Sico van der Meer

DECEMBER 2016

Medium-sized states in international cyber security policies

Some medium-sized states play varying, yet important roles in international cyber-security policies. This Policy Brief offers a concise overview of five medium-sized states with such a prominent position. How did these states attain these positions, and what are the benefits and challenges? The analysis shows that these positions are not easy to acquire or to maintain. Whilst the will to continuously invest and to develop an integrated (whole-of-government) approach seems to be an obvious key requirement for success, cyber security as a policy area is very broad. Remaining in a lead position may require looking for 'a niche within the niche'.

Cyber security is a 'hot issue' in international politics; the rise of cyber-espionage, cyber-manipulation and cyber-warfare capabilities is a global reason for concern. Yet, some states are more active on this issue than others. Especially the big powers in international relations like the United States, China and Russia have developed impressive (offensive and defensive) military and intelligence cyber capabilities. Some smaller states, however, are playing a more than an average role in international relations regarding cyber security as well, for example in diplomatic activities relating to this issue.

This Policy Brief offers a concise overview of five medium-sized states with such a prominent position. It will show that they acquired their position in different ways, and will analyse the benefits and challenges related to (maintaining) their position. The Policy Brief concludes with a few lessons for medium-sized states aiming to play a more than average role in international cyber-security policies.

Cases and method

This publication will analyse the policies of five medium-sized states with a more than average position in the international cyber-security policies domain – with an emphasis on international, because many states invest in domestic cyber security without much international resonance. To facilitate a comparison, only democratic states are selected for this brief analysis, thus excluding authoritarian medium-sized states like Iran and North Korea which have a strong international cyber-security position as well. In alphabetical order, Australia, Estonia, Israel, the Netherlands and South Korea are selected as cases because of their – to some extent – comparable international political weight and position in the international cyber-security domain. One may posit that Estonia is rather a small power when compared to the other selected medium-sized powers, but as will be described below, especially in cyber policies its position stands out more than that of other small states.

Without any claim of being exhaustive, this selection of countries will provide an insight into medium-sized states' policy dilemmas regarding the development and maintenance of prominent positions in international cyber security. The analysis is based upon a literature review as well as various interviews with experts and policy makers. Because most of the interviews took place on the basis of anonymity, no references to the interviews themselves are made.

Australia

The Australian government started investing in a regional leading position in cyber security in 2009, when its first Cybersecurity Strategy was published. A new version followed in 2016, and together with the Defence White Papers published in 2009, 2013, and 2016 as well as the National Innovation and Science Agenda, it initiated integrated policy efforts regarding cyber security. The government aimed to increase the security of Australian cyber networks in order to reduce the risks of cybercrime, espionage and online disruption with the assumption that this would also strengthen the Australian economy, attracting more foreign economic activity to operate from this digitally 'safe haven'. Next to national security and economic profits, foreign policy benefits were incorporated as well: Australia considered cyber security to be a new niche by which to gain more regional influence. By combining its aspired forerunner's role with capacity-building efforts in neighbouring states, it hoped to create better relations with countries in the region, which in turn would further increase positive effects on the economic and security situation. Cyber security was thus considered as a policy area from which Australia could benefit in many ways.

In the years following 2009, massive financial investments in cyber security ensured the creation of a comparatively secure cyber environment. Military cyber capabilities also increased; Australia is exceptionally transparent on possessing offensive cyber-weapon capabilities. The investments also stimulated cyber innovation, especially because of the strong focus on multi-stakeholder involvement in these efforts. Public-private cooperation was prioritised from the start, although voices from the side of industry have been critical; in practice a coordinated, whole-of-government approach was lacking and defining the respective roles of government and industry needs to be improved.

So far, it is difficult to measure the economic effects of the cyber-security investments; no figures are available indicating whether Australia has actually attracted more foreign money because of such investments. Moreover, while Australia made a considerable leap in securing its cyber infrastructure after the investments started in 2009, a few years later other regional powers like Japan and South Korea were reported as having already overtaken these cyber-security levels once more.

From a foreign policy perspective, the aim to use the upgraded position in cyber security to engage countries in the region has also been criticized. A concrete strategy of how to actually achieve this goal is lacking. According to one analysis little has been achieved and "Australia missed a golden opportunity to influence regional thinking on cyber-matters." The main problem seems to be that whilst the plans appeared to be effective on paper, their implementation should have received more attention.
In particular in the areas of cooperation and coordination between various parts of government improvements are required. In 2016 the functions of a Minister for Cyber Security and an Ambassador for Cyber Affairs were created to (better) coordinate Australia's cyber efforts domestically and internationally.

Estonia

Estonia's prominent role in international cyber-security policies is defined by two factors. First, the government started investing in digital government and e-services and their security relatively early in 1995. In 2005 Estonia claimed to be the first state in the world to hold elections via the Internet. This trend towards increased and secure digitalization has continued ever since. According to the governmental Digital Agenda 2020, "The goal for Estonia is to maintain its image as a technologically advanced country and well-developed information society. This would support the efforts of our businesses in foreign markets, contribute to attracting foreign investments and help Estonia to achieve its general foreign policy goals."

A second reason for Estonia's prominent position is the fact that in 2007 it was the first state in history to experience a large-scale cyber-attack. The massive Distributed Denial of Service (DDoS) attacks disabled many governmental and banking websites. The cyber-attack was most probably instigated by Russian (state and/or non-state) hackers after tensions regarding a Soviet-era statue and the position of the Russian minority in Estonia. Although the cyber-attack did not cause any serious harm, it put Estonia in the international spotlight, highlighting the risks related to cyber activities. The attack also raised the awareness of the Estonian government about the downsides of digitalization, and it became internationally vocal on cyber-security risks and the need for increased cyber-defence cooperation. Being a member of the North Atlantic Treaty Organisation (NATO) and the European Union (EU), Estonia's experience resulted in a leading role in the process of developing NATO's first cyber-defence policy in 2008. The country also contributed to various EU initiatives regarding cyber security.

According to some researchers the Estonian government successfully used the rather limited cyber-attack of 2007 to gain publicity for its cyber-security policies. Estonia became the host nation of the newly-established NATO Cooperative Cyber Defence Centre of Excellence. This Centre also initiated the Tallinn Manual Process, an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare which is generally considered to be a pioneering contribution to increasing international understanding and clarification of how international law should be interpreted in the cyber domain.

Considering its small size (1.3 million people), the government's policy aim to brand Estonia internationally as "a world-renowned e-state" is effective. According to some researchers, Estonia successfully uses its cyber-security position in its foreign and security policy by projecting a combination of soft power (winning friends and increasing visibility and influence) and hard power (enforcing deterrence against potential bigger enemies).

Yet, a problem for Estonia is that while the country started from a rather unique position, in the meantime various other states have embraced the same niche as well. Estonia's niche of raising awareness for the need of international cyber security cooperation thus made it a victim of its own success: bigger states with more capabilities (also in the number of people) are taking over Estonia's role to some extent. More international attention means more international meetings, and a small country like Estonia is losing influence because it cannot attend them all. In this way, its prominent position is slowly diminishing. According to some interviews conducted for this Policy Brief, Estonia tries to deal with this problem by focusing even more on the regional level (the EU and NATO) instead of the global, multilateral level.

Israel

In the last couple of decades Israel has invested strongly in its military cyber capabilities, not least because Israel's government and military are under constant cyber-attack from (non-state or state-sponsored) hacker groups originating from hostile countries in the region. The Israel Defence Forces' Unit 8200, specializing in electronic intelligence operations, gained the reputation of being one of the most advanced and powerful cyber-warfare organisations in the world.

Among conscripts this military unit is a very popular one, which allows the most capable young software engineers to be selected for this unit during their period of conscription. This not only enables continuing innovation and strengthening the quality of the military unit, but also has an impact on the Israeli economy. Most of these conscripts return to civil society after their military service, with a great deal of added expertise in cyber security. In the past decade, many of these former conscripts have started new companies in cyber security, especially focussing on leading-edge technologies for military and intelligence applications (this specific focus is why the general public has never heard of these companies). In 2015, Israel exported cyber-security technology to the value of 3.5 to 4 billion US Dollar, some 5% of the global cyber-security market. Some 20% of Israeli high-tech companies are engaged in cyber security, resulting in it being the country's biggest economic sector.

Israel's military and economic position in cyber-security technology development mainly resulted from government investments in this area, which started relatively early compared to other governments (probably already in the 1980s, but at least in the early 1990s). Moreover, it has been a coordinated whole-of-government approach, involving especially military, educational and economic policy measures. While the Israel Defence Forces invested in military cyber capabilities, the Ministry of Education set up after-school programmes for middle and high-school pupils to learn about cyber-security engineering. These programmes interacted with the increasing popularity of conscription within Unit 8200. Furthermore, the government has identified cyber security as a key driver of economic growth, stimulating (start-up) companies in this sector with tailored beneficial policies. To explain the success of this mix of military, educational and economic policies, it should be mentioned that Israel is a rather unique country considering that its military is a much larger part of its economy and, with the three-year period of compulsory military service, the military's effect on society is also much greater compared to other countries.

The Israeli advance in military cyber capabilities seems to be rather stable, considering the ongoing massive investments in this area. However, there are some concerns in Israel that the economic growth in this niche market cannot continue forever. While new companies are still entering this booming market with a relatively high frequency, some experts warn against a 'cyber bubble'. And even though one might safely predict that the global demand for cyber-security technologies will not soon diminish, Israel is a relatively small country and there is a risk that bigger firms, especially from the United States, will take over the smaller Israeli competitors and thus reduce the Israeli role in this area. On the other hand, this has not happened to Israel's successful conventional defence industry either, so this fear may be theoretical to some extent, especially considering the continuing flow of new cyber-security experts ending their conscription – something with which the US cannot compete.

The Netherlands

The Netherlands' prominent role in international cyber security is relatively new and builds on an integrated policy agenda as well as the country's traditional role as a bridge-builder in international diplomacy. The Dutch focus regarding international cyber-security policies is mainly on international cooperation and dialogue, including capacity-building efforts to assist other states in strengthening their cyber environment. For example, the Netherlands organized the fourth Global Conference on Cyberspace in 2015, and co-initiated the Global Forum on Cyber Expertise (GFCE) aimed at international cyber capacity-building. Dutch diplomats are very active in international fora like the United Nations and the Organization for Security and Co-operation in Europe (OSCE) to enhance constructive discussion on the interpretation of international law regarding cyber security and on the creation of non-binding norms and confidence-building measures. The Netherlands also initiated The Hague Process, together with the NATO Cooperative Cyber Defence Centre of Excellence, to ensure the transparency of the process to create a Tallinn Manual 2.0 on international law and cyberspace.

From a military perspective, the Dutch government invests in developing increased cyber intelligence and warfare capabilities.

Although many countries are doing that the same, the Netherlands is rather unique (like Australia) in its transparency with regard to its offensive capabilities. Economically, the Netherlands aspires to be one of the leading ICT countries as well, promoting innovation in the cyber domain and branding itself as 'the digital gateway of Europe'. This positive image is also meant to attract more economic activity from abroad, although it is not quite clear how much this cyber image contributes in that regard.

One of the key features of Dutch cyber-security policy, both on the political and economic level, is its focus on the multi-stakeholder approach. On the national level this approach is embodied in the coordinating organisation for cyber security: the National Cybersecurity Centre is not a government-only body, but a so-called public-private partnership, in which a variety of stakeholders are represented. In policies like diplomatic and capacity-building efforts the multi-stakeholder approach is also given much attention.

A problem in defining how the Netherlands established its relatively prominent position in international cyber-security policies is its broadness. As some interviewees mentioned: the Netherlands is active in many international fora regarding cyber issues, but for outsiders a clear focus is hard to identify. Does the Dutch cyber niche involve economic innovation, capacity-building, privacy and online freedom, the multi-stakeholder approach, or international norm-setting diplomacy? Whilst the broad focus is positive for the international visibility of the Dutch activities in the cyber domain, and thus contributing to the image of the country as being 'cyber-minded', one might wonder whether the Netherlands will at some point experience a similar problem as Estonia: how to guarantee enough capacity (especially in personnel) to ensure an active involvement in the huge, and still increasing number of specialized international fora in the cyber domain. The lack of a clear focus within the international cyber-security policy area may also increase the risk that the Dutch prominent position in any or all of these areas will be overtaken by other countries that are able and willing to invest more efforts in certain specialist issues.

South Korea

South Korea had a similar experience to that of Estonia with the government focusing on high-tech innovation and the digitalization of its society and economy, as well as a relatively early large-scale cyber-attack in 2009. In this case, the attack against computer networks of government and financial organisations is generally attributed to North Korea, which allegedly also conducted several other cyber-attacks against South Korean targets in later years.

These attacks resulted in South Korea also becoming vocal concerning the need for international cyber-defence cooperation. The South Korean National Cybersecurity Action Plan from 2011 advocates international cooperation on cyber defence and deterrence, and to some extent also favours a multi-stakeholder approach, although with clear state coordination. In recent years South Korea has envisaged itself as being a so-called Middle Power, functioning as a 'broker' in the international community to enhance multilateral cooperation regarding (among other issues) cyber security. With the aim of attaining this broker position it organized, for example, the third Global Conference on Cyberspace in 2013, as well as the yearly Seoul Defense Dialogue (SDD) meetings in which cyber security is a prominent topic.

From an economic point of view, South Korea has already positioned itself for some decades as a country of technological innovation, although not specifically being cyber-focused. From a military perspective, the South Korean National Security Strategy includes the use of proactive or pre-emptive (read: offensive) cyber-defence strategies as well.

However, notwithstanding the aim of becoming a broker in international cyber-security policies, in practice South Korea focusses its cyber-security policy to a large extent on bilateral cooperation with its main ally, the United States. According to some experts, this close relationship damages South Korea's international position. Some countries may question South Korea's independence in this area, thus limiting the country in playing the role of a 'broker' in international cyber-security issues.

Apart from the bilateral focus on the US, South Korea's cyber-threat perception is perceived to have a limited focus on one specific adversary: North Korea. While this is indeed understandable, this focus is not shared by many other states, thus limiting the potential added value of South Korea's cyber-security strategies for other countries. Last but not least, South Korea is facing a problem which is comparable to that of Estonia. While its prominent position in cyber-security policies was partly established because it was one of the first countries to experience a large-scale cyber-attack, in recent years many other countries have experienced similar attacks and South Korea's position has become less unique in this regard.

Conclusion

In the five cases described above, two main incentives can be noted for countries to attain a prominent position in international cyber-security policies: experiencing large-scale cyber-attacks (Estonia, Israel, and South Korea) which motivated countries to invest in cyber-security policies, and deliberate choices to focus on this policy area (Australia and the Netherlands). Whereas the first incentive allowed for some 'authentic' visibility, the second approach involved creating some sort of 'cyber reputation'; Australia and the Netherlands had to build this reputation almost from scratch. For both trajectories for becoming a prominent player in the field of international cyber security it can be said that maintaining this position is not easy. Having a position as a result of an attack provides no long-term benefit, nor can any deliberate investment guarantee such an outcome. Australia is an example in which governmental investments in a secure cyber environment provided a huge stimulus to its position, but a few years later experts already warned that other countries had overtaken Australia. Endurance is required and, in that sense, endurance resulting out of a perceived national security need seems to be the most promising for maintaining a noticeable role.

Two important steps appear to be relevant for states that aim to effectively attain an international prominent position in cyber security. First of all, investments in cyber capabilities are necessary. The key seems to be the role of the government in stepping up its own investments in securing cyber infrastructure (and to some extent, investing in military and intelligence cyber capabilities). Second, an integrated approach makes efforts potentially more successful and maintainable. This requires not just investments, but also economically beneficial regulations for cyber-security firms, building adequate qualified personnel capacity within the government, as well as a whole-of-government approach including public-private partnerships. In all five cases military, economic and diplomatic efforts were combined, although in some cases more successfully than in others. Israel offers the clearest example of combining military investments with educational projects and economic regulations in order to create a fruitful environment for cyber-security activities.

The benefits of a prominent position in international cyber-security policies seem clear: such a forerunner's role may strengthen a state's soft power (winning friends and increasing visibility and influence) as well as hard power (deterring potential enemies). For some states, cyber security may offer an approach to strengthen existing 'niches'; Israel has done this in the military domain and the Netherlands has bolstered its diplomatic bridge-building reputation. Whether investments in international cyber-security policies attract impressive foreign economic investments is not yet clear; reliable data on this topic have not been found. One could argue that extra international visibility in a positive way will always contribute to the economic attractiveness of a country, but considering the necessity of ongoing investments as well this interrelationship requires a more in-depth study.

An important question is also whether a prominent position in cyber security can still be built in an environment where more and more states are heavily investing in this issue. Related to this question is the underlying motivation for doing this – is it out of a perceived security need, or for claiming a role in international fora where cyber security issues are discussed in a very fragmented way. The latter is, obviously, a choice driven by the need for diplomatic visibility – which in turn may enhance international political and economic relations. Both may be valid arguments, but the first is a choice out of perceived necessity and, realistically, is easier to maintain.

Yet, as the case of Estonia suggests, even the first reason requires substantial investment, especially if the aim is to expand a country's role and to participate in the many international meetings in the cyber-security domain. This is a challenge for all countries, but in particular for those medium-sized states that want to play a prominent role. Similarly, a broad approach, such as that adopted by the Netherlands, requires either huge numbers of staff and broad expertise, or it runs the risk of spreading its role and visibility rather thin. Here, smaller countries are also challenged more than bigger countries.

Considering the findings of this analysis, countries aspiring to achieve a prominent role in cyber security may benefit from zooming in on smaller issues, or seeking 'a niche within the niche'. A case in point is Israel, which created a niche in cyber technologies for military and intelligence operations. Another example is Estonia trying to rebalance its niche to focus mainly on NATO and EU cyber policies. Countries like Australia and the Netherlands may also have to choose a more specific focus in order to retain the niche position that they have developed. Considering that they are currently focusing on a relatively broad spectrum of cyber-security aspects, it will take high investments and personnel capacity to maintain a leading role in all of them. Operating in coalitions of like-minded states, in which a division of tasks is possible to some extent, may be a practical solution as well.

Another aspect that can help medium-sized countries to play a meaningful international role is their (relative) independence. Too much focus on certain bilateral ties may be damaging, as can be seen in the case of South Korea where close ties with the United States could harm its desired position as an independent 'broker'. On the other hand, Israel is also a very close ally of the US, but for its niche position of developing and selling military and intelligence cyber technology this close alliance is less relevant because it is not claiming any independent 'broker' role.

Finally, this concise analysis shows that for medium-sized states attaining and maintaining a prominent role in international cyber-security policies is not an easy challenge. The will to continuously invest and to develop an integrated whole-of-government approach is a key requirement for success. Moreover, even within the cyber-security niche itself, broadness may be a risk and looking for 'a niche within the niche' might be beneficial. Last but not least, the benefits of a prominent position in international cyber-security policies, especially strengthening both the soft and hard power status of the state, are difficult to measure directly.

About the Clingendael Institute

The Netherlands Institute of International Relations ‘Clingendael’ aims to enhance and deepen knowledge and opinion shaping on issues related to international affairs. The Institute realizes this objective through its research, training and consultancy for national and international parties. The Institute publishes reports and policy briefs, holds numerous conferences and publishes the digital magazine Internationale Spectator. Every year Clingendael offers a wide spectrum of courses and programmes, training hundreds of diplomats, civil servants, and other professionals from all over the world. For further info, please view: **www.clingendael.nl**

Follow us on social media

@clingendael83
The Clingendael Institute
The Clingendael Institute

About the author

Sico van der Meer is a Research Fellow at the Clingendael Institute. His two research topics are Weapons of Mass Destruction and Cyber Security, both from a strategic policy perspective.