The Hague Centre for Strategic Studies

Vaste commissie voor Justitie en Veiligheid
Postbus 20018
2500 EA Den Haag

Office Address
Lange Voorhout 1
2514 EA The Hague
The Netherlands

t +31 70 318 48 40
f +31 70 318 48 50
w www.hcss.nl

Date
16 February 2018

Subject Transcript en notities van Dr. Alexander Klimburg's deelname aan het Rondetafelgesprek Cybersecurity van de Vaste Commissie voor Justitie en Veiligheid in de Tweede Kamer te Den Haag op 7 Februari 2018.

On the request of the Chairman, please find below the transcript and speaking notes of Dr. Alexander Klimburg's testimony made to the aforementioned Commission during the Cybersecurity Roundtable on 7 February 2018 in The Hague

Part I: First intervention

Alexander Klimburg: "It is my pleasure to be here today, and a distinct honor to be the only foreigner invited to provide their views on the development of the Dutch national cyber security policy. To provide you with a brief overview of my background – for the last couple of years I have acted as a program director at *the Hague* Centre for Strategic Studies (HCSS), and have been a fellow and faculty affiliate at Harvard University. I remain a non-resident senior fellow at the Atlantic Council in Washington DC and I am affiliated with an Austrian think-tank. Within my function at the HCSS I am currently the director of the Global Commission on the Stability of Cyberspace (GCSC), which is a blue-ribbon commission of notable individuals that was launched with strong support of the Dutch Ministry of Foreign Affairs and which is now working on new norms and policy initiatives that help advance international peace and security in cyberspace.

Having read many of the comments that were submitted in advance, I can say that I am in strong agreement with most of what has been submitted to this Commission. Although I have never lived in The Netherlands, I have followed Dutch cyber policy closely since a number of years. I was asked to provide my input on the first Dutch national cyber strategy in 2011 and indeed since then have worked with a wide range of governmental actors on issues surrounding national cybersecurity strategies and international approaches to cybersecurity. Having worked closely with over a half dozen governments in Europe and North America and published widely on the subject, I would like to share what I consider to be the **two clear strengths of the overall Dutch approach to cybersecurity**, and how you may consider building on this strength. Thy are of great importance to a country with the second largest Internet Exchange point of the world (AMS-IX) and a digital economy that accounts for close to 23% (€158,01bn) of its GDP.

The first immutable Dutch strength in national cyber security is an unparalleled understanding of what it means to engage in a so-called **"whole of nation" approach**. This is a term that is often easily confused with the "whole of government" approach although there is an obvious difference (except in the case of China). While in a WoGA the key issue is one of coordination, of managing obligations and duties set out in law and carried out by the executive branch of government, the WoNA is a lot messier. It involves the cooperation with many non-state actors, which partially can be structured through legal measures, but most likely will need to have the willingness and basic volunteer spirit to work. WoNA ideally does not rest upon legal coercion and the threat of punishment alone, but in the best case is motivated by the willingness of the non-state sector to accept not only the legal but also the moral legitimacy of governmental efforts. Basically, it rests upon the power of attraction – a term that Joseph Nye at Harvard called soft power. To get to this level of cooperation, the government must, therefore, continuously be perceived as "doing the right thing".

Doing the right thing is not really a question of ideology, but of basic smarts. For instance, most would not dispute if government has a legitimate right to explore offensive cyber measures, either for those capabilities indicated in the setting-up of the MinDef Joint SIGINT Cyber Unit, or indeed the provisions outlined in the new Intelligence and Security Services Act (the WIF). It is really about making sensible choices, like for instance separating the job of the defenders from that of the shooters, or cyber-warriors and cyber-spies. While for instance the job of the attackers is certainly made easier by merging the two functions, there are some better technical reasons to have this function together, the potential loss of trust with the non-state actors is potentially catastrophic. How could it not be, if the defenders have to worry that the State might be pursuing other interests then simply those of helping the companies protect their network? These companies already play a vital role in many more voluntary powerful *Whole of Nation* coordination instruments that are necessary both in strategic planning and operational execution. For instance, according to my understanding, the little-known NCO-T group that coordinates the telecom operators and the government is also the key body that would help provide private sector expertise to the so-called *Incident Respose Board*, a crisis management instrument that can provide crucial input into national crisis management, and which is internationally considered a novel idea. The Cyber Security Council, which played an important political and strategic advisory function already during the first major cyber crisis, the DigiNotar incident in 2011, is another such example.

WoNA also helps contribute to a perennial problem. Namely, how to improve the Whole of Government coordination. The NCSC is internationally considered to be the best-in-class response structure, and, as there is a general commitment to this type of model, it is positive that the NCSC may in the future be freed to concentrate more on its fundamental operational tasks, leaving the NCTV and other involved agencies to be able to develop longer-term strategies. While it remains fundamentally important that the NCSC, as operators of the NDN and similar WoN defenses, remain a civilian institution, there would be a stronger benefit in bringing together, perhaps at a higher level or even within the NCTV, an intelligence sharing center that can combine more fully the civilian, military and intelligence view of threats in cyberspace. Whichever agency assumes responsibility for the operational and strategic cybersecurity tasks, it is paramount for it to be connected with a true budgetary authority, as otherwise the ability to respond is limited.

Finally, the Dutch tradition towards WoN will also help to address some of the most difficult issues facing all developed nations: what is the acceptable level of burden to impose on companies with questions of liability in the fore? How can education be conducted, both horizontally but also vertically, to make sure that the electorate as well as the decision makers, such as yourself, are adequately appraised of some of the most important need-to-knows? And finally, what are the appropriate responses to some of the more visible cyber attacks that are the same as information warfare attacks, which directly go to the hearts of our democratic societies? How can our societies and our governments become more resilient to these threats, which are multifaceted, and sometimes not even of malicious intent – cables can get cut, for instance – and require all hazard risk-based response? These questions will not be answered easily or quickly, and, therefore, I applaud the motion that was introduced in the Second Chamber on 5 September 2017 to provide additional funds for research and development of cybersecurity.

Secondly, I would like to highlight what I and many other foreign observers consider a particularly strong part of the Dutch approach – and that is **commitment to rights.** Many of the issues that we deal with on the cybersecurity side are aspects of underlying weakness of Cyberspace. In cyberspace, unlike the other domains (air, land, sea, space), humans determine the physical rules - we say what gravity is. When our wishes change, the domain changes. There is one major disclaimer in this regard: cyberspace is not run by governments. The civil society writes most of the code, the private sector owns nearly all of the infrastructures. Governments can only attack parts of cyberspace, but they don't build much in it. This is likely why it has been such as success so far. While countries like Russia and China would very much like to have an intergovernmental Internet, western democracies have committed to a non-state Internet, and rightfully so. This does not mean that government attempts to get involved are unwelcome, but they have to be careful to not imply that the Internet is in fact a state edifice. Like the seas, it belongs to everyone.

Instead of more laws, the solution is partially one known for over 400 years to many Dutchmen – peace and profit require commonly accepted principles. Ever since Hugo Grotius defined the “*mare liberum*”, Dutch policy has been keenly aware of the importance to establish international defined rules of the road for all to follow. In technical terms, this means supporting the open standards and other important technical research that underpins the Internet. But at the political level this means committing to a process of international state and non-state norm building that provides rules for everyone to follow. The Hague Centre for Strategic Studies houses the Global Commission on the Stability of Cyberspace to this end - an initiative heavily backed by the Dutch Foreign Ministry that helps play a vital role in defining these international norms and policy initiatives. But the most important norms are those that are set by the governments themselves. This Commission has already shown with this meeting that it fully understands the importance of a multi-stakeholder process, and I applaud you for showing not only the Netherlands but also the world how these type of consultative processes should be done. “

Part II: Second Intervention

Van Dam: “First of all, I have the impression that you have much more to say than we gave you opportunities to. So, perhaps you can give us your paper afterwards; I would be interested in that. Another point is that you wrote a book on cyber security **[*"The Darkening Web: the War for Cyberspace”* published by Penguin]** and, well, I have the impression that you can look from the outside to our country and can you give two recommendations on what point we could improve on the subject of cyber security?***”***

Chairman: “Maybe I can directly add my question to that because it is on the same level. I was interested in international comparison. Which countries – for example, countries in the European Union or even in the whole world – are doing very well and what can we learn as the Netherlands from them? So, I think we can bring those two questions together and give you the possibility to share some thoughts with us about this.”

Alexander Klimburg: “So, thank you for those questions. The risk of asking two questions to a cybersecurity expert is that you will get three answers. So, I will try to provide you with two and a half answers if possible.

First of all, just in terms of comparisons with abroad – obviously, sometimes it is difficult – different countries, different systems. However, I think there is one thing to keep in min, namely that some of the best practices that have been quoted often indicate it is important to overcome departmental silos. So, if we look at, for instance, the experience in the UK, which is a more centralized system than the Dutch system, they have highly centralized efforts around the cabinet office and most importantly this means disbursement of funds, essentially. So, individual departments keep their money, but they have additional top of money that is disbursed from the cabinet office. I do not think the argument we are talking about, whether departments have similar authority here, that is for you to figure out, but there is a general agreement that it is needed to have centralized authority to have a budget to deal with the issue of overcoming silos because we only have issues where an organization like the NCSC, which is incredibly important operational organization, does not have a very large budget, needs to either concentrate on its operational task, but at the same time it has potentially a wider contribution yet to be established in terms of providing input into a common intelligence picture. So, this is the second recommendation I would make.

There is a drive towards sharing a common threat picture that effectively brings together what you would have as the input from the special services, from the military community, the diplomatic community because a lot of the signals that we receive in cyber are effectively in done in a political context and this should not, in my impression, be given to the NCSC, which should be free to do its operational job, but maybe in a different intelligence sharing body, which should be able to bring these things together without contaminating some of the important non-state relationships.

Second of all, in terms of how outreach works and particularly your question about how to increase the interaction between state and non-state actors. So, first thing to be said is the Dutch approach is considered to be very close to be the best in class. To take the WIV – the process what was part of the intelligence act that was debated – the only country that has had a similar process has been the Swedish approach – the so-called FRA law. FRA is their Signal Intelligence Agency, which in 2006 and 2007 went through a similar open consultation process that you had in the Netherlands. It does not have all the oversight bodies that you have defined in the WIV, like the TIP Commission or the CTVID, which is unique and which even the Swedes do not have and absent of any ideological reservations that we have about cyber intelligence. This is a very open process that is fairly unique. The challenge is to go forward on how you reach out and how the advocate on this policy work together with other organizations: getting the labour unions, the employment unions, the representation of the civil society and private sector on board and effectively advocate for it if that is your goal. That is part of the challenge and many governments have obviously failed in this last step. So, that is indeed a challenge.

Finally, just to get to the educational components, because that was asked beforehand. So, building capacity is not only a horizontal challenge, but also a vertical challenge. You do not only want to educate the civilians / the electorate on the basic cyber hygiene. You also want to educate, for example, the specialists, such as the military cyber operators to learn about Internet governance; the diplomats need to learn about cybercrime; and of course the political decision-makers, such as yourself, need to be regularly informed about the topics that are being debated. So, Australia and the UK have executive programs in this regard; Sweden and Switzerland have established similar programs. I would encourage that as part of the security initiative that was mentioned last year, but you go a little bit further. So, in the United States for instance, the so-called Sputnik Shock led to a massive investment in the hard sciences. The Netherlands has had the benefit of many different cyber shocks. I would say, maybe this is the chance to invest in a massive cyber education program and do not let a crisis go to waste."