Prioritising Denmark’s Cyber Policy

Denmark Should Avoid a ’Digital Geneva Convention’

By Jeppe Teglskov Jacobsen, PhD Student, Danish Institute for International Studies
Prioritising Denmark's Cyber Policy
Brief by Jeppe Teglskov Jacobsen,
PhD Student, Danish Institute for International Studies

Copenhagen December 2017

© Royal Danish Defence College

All rights retained. Mechanical, photographic or other forms of reproduction or copying of this brief or parts thereof are permitted solely by prior agreement between Danish Defence and Copy-Dan. Every other use without the written approval of the Royal Danish Defence College is prohibited by Danish copyright legislation, with the exception of short excerpts for use in reviews.

Royal Danish Defence College
Ryvangs Allé 1
DK-2100 Copenhagen
Denmark
Phone: +45 728 17000
E-mail: fak@fak.dk
Editor in Chief: Jens Ringsmose, Head of Institute for Military Operations
Internal peer review
Layout: Royal Danish Defence College
ISBN: 978-87-7147-212-7
## TABLE OF CONTENT

- Denmark Should Avoid a ’Digital Geneva Convention’ ........................................ 4
- Who Can Be Blamed for WannaCry and NotPetya? ........................................... 5
- Pandora’s Box ........................................................................................................ 8
- Existing Diplomatic Channels ................................................................................ 9
- Conflicting Security Concerns ............................................................................... 11
- Enforcement Problematics ................................................................................... 12
- Denmark’s Political Latitude .................................................................................. 13
  - Cyber Diplomacy .................................................................................................. 14
  - Better Regulation of the IT Sector ........................................................................ 14
  - A Stronger Cyber Protection ................................................................................ 15
- Conclusion ................................................................................................................ 15
Denmark Should Avoid a ‘Digital Geneva Convention’

Even though Denmark has an interest in better IT security and legal transparency in cyberspace, it is not in Denmark's interest to open negotiations on a broad digital convention on the behaviour of states in cyberspace. Still, greater prioritisation of Denmark's cyber diplomacy is necessary.

We have recently seen a marked increase in the number of incidents where criminals using malware have encrypted companies’ computers and demanded a ransom for releasing the encrypted data to the companies. This hostage-taking technique known as ransomware really caught the public eye in May 2017, when the British National Health Service suffered under the worldwide WannaCry Attack. When a month later Maersk experienced extensive disturbances caused by a similar attack, i.e. NotPetya, the threat also caught the attention of the Danish public. The incidents seem exceptional because they involve techniques for exploiting IT vulnerabilities developed by the National Security Agency (NSA), and because these vulnerabilities were leaked in April this year. In continuation hereof, the NSA has been severely criticised for having developed and stored techniques that make civilians and private companies vulnerable to attacks. Especially the private sector has criticised the NSA, arguing that the agency should cooperate more closely with e.g. Microsoft to make cyberspace as safe as possible.

Based on this critique, Microsoft’s President and Chief Legal Officer, Brad Smith, had suggested – even before the WannaCry Attack – that a ‘digital Geneva Convention’ be developed, a suggestion that has subsequently been met with great public support.1 Briefly, Microsoft’s proposal for a digital convention contains the following elements: 1) a ban preventing states from compromising private companies and critical infrastructures, 2) an injunction forcing states to cooperate with the private sector on identifying and tackling IT vulnerabilities and cyber incidents, and 3) a restriction of states’ rearmament of cyber weapons. In fact, Smith’s use of ‘Geneva’ here is slightly misleading, as Geneva conventions typically and exclusively regulate wars, not states’ behaviour in general. Smith’s proposal for a digital convention is thus more than a measure to regulate cyber conflict, and it encompasses a disarmament agreement and civil-military collaboration. A ‘digital convention on the behaviour of states in cyberspace’ would thus have been a more accurate and less bewildering title than a ‘digital Geneva convention’2 – but perhaps also less catchy.

This does not change the fact that a small state like Denmark as a rule will benefit from more legal transparency at international level on the behaviour of states in cyberspace. A legal

---


Prioritising Denmark’s Cyber Policy

framework is *de facto* the best tool for small states to hold large states liable for their actions. The widespread use of IT also means that Denmark has an interest in ensuring that products from e.g. Microsoft, Siemens, Apple and IBM are as safe as possible because an improvement of the general level of IT security will limit other states’ ability to spy on and attack Denmark in cyberspace. However, negotiations on a general convention on the behaviour of states in cyberspace are not necessarily the most desirable approach, seen from a Danish perspective. In this brief I will discuss the four main reasons for this:

1) A negotiation process under the auspices of the UN will in all likelihood result in diplomatic discussions on issues that Denmark does not wish to reopen.
2) A negotiation process risks undermining existing formal and informal discussions on international law in cyberspace.
3) A negotiation process will in all likelihood founder because a number of states will refuse to abstain from utilising IT vulnerabilities to catch criminals, prevent terrorism and conduct espionage in general.
4) A digital convention on the behaviour of states in cyberspace is difficult to enforce.

These arguments do not mean that Denmark should refrain from acting, though. Toward the end of the brief, I suggest that the Danish government should strengthen its efforts within foreign, defence and business policy.

Who Can Be Blamed for WannaCry and NotPetya?

Before we look at potential challenges facing a negotiation on a convention on state behaviour in cyberspace, it is worth considering who may be blamed for the ransomware incidents in spring and the insufficient IT security in general. This will highlight the fact that Smith’s proposal for a convention only addresses one selective part of the problem.

The actor who has been the subject of most criticism in connection with the ransomware incidents is the NSA. The NSA discovered a flaw in Microsoft Windows, developed techniques to utilise this flaw and stored or used the technique in its retrieval work. It is difficult to criticise the NSA for doing the job it was set up to do. Nevertheless, a number of things mean that the NSA does not get off the hook that easily. First and foremost, it is unclear whether the IT vulnerabilities that were exploited have actually been subjected to the US procedure which shall determine whether a vulnerability should be saved or shared for remediation. As the procedure is classified, it is impossible to find out how useful the technique really was for the NSA’s signal intelligence efforts. Thus, for now this criticism founders here. It is easier to blame

the NSA for its inability to avoid leaks. Brad Smith compared WannaCry to a situation where the US military loses a Tomahawk missile.\(^5\) However, this analogy does not mean that there is necessarily a need to remove Tomahawk missiles or cyber weapons from the US weapons arsenal, as insinuated by Smith, but rather a need for more and better control and security in connection with the NSA’s storage.

The NSA is far from the only player who may be blamed for the ransomware incidents. It is obvious that cybercriminals and Shadow Brokers, the group that leaked the NSA techniques, also play a key role. However, it is even more interesting that Microsoft, the affected companies, their associated IT administrators and ultimately various governments may also be blamed for the fact that e.g. ransomware has developed into the serious security challenge as is the case. Today, the majority of companies depend on IT systems. That is not a problem in itself. The problem arises when those very companies at multiple places in their IT infrastructure have old and no longer supported operating systems, such as Windows XP, installed on their machines. Or even worse: when the IT administrators have not installed updates for their existing systems. The WannaCry episode is an example of this: About six weeks before the WannaCry incident, Microsoft had released an update to its supported operating systems, which rectified the mistake that the NSA had probably utilised until then. In other words, companies learned in the hard way that a more thorough understanding of and investment in own IT infrastructure is necessary if you want to minimise the risk of ransomware and other more serious cyberattacks.

However, even major investments in IT security never completely protect a company from cyber thefts and interference, the reason being that software will rarely perform exclusively as intended by the programmer or administrator. Programming and installing IT systems is a complex task and users of IT systems are often careless when dealing with attached files, links and the like. Thus, it is almost impossible to prevent outsiders without authorisation from accessing or affecting an IT system.

This means that the IT companies which develop many of the operating systems, applications and hardware that we currently rely are also partly to blame. Microsoft programmed the malfunctioning code utilised by the NSA and the persons behind WannaCry and NotPetya. As opposed to what applies within the pharmaceutical and automobile industry, software companies have no legal responsibility for ensuring that the product they market is safe. This means that Microsoft has developed a business model that continually sends new operating systems on the market and only updates new products, failing to update old, malfunctioning systems. This contributes to the magnitude of the problem. It raises the question whether

---

Microsoft should be blamed for not adequately protecting the customers to whom the company sold its products, but who cannot afford to invest in the latest supported operating system.

Brad Smith's wish for a digital Geneva Convention to protect civilians from the unauthorised use of cyberspace by states may be viewed from a different perspective than presented by Microsoft. A digital Geneva Convention in the form envisioned by Smith represents just one version of reality. This version ignores the fact that Microsoft, Google and other tech giants will still only have an incentive to invest in the remediation of errors and vulnerabilities if they believe that it will increase their overall economic profit. With no state compromising of their IT systems, the big tech giants have less incentive to develop techniques and practices that make programming better at the first onset. In addition, the companies' profit margins must be considered. Several tech companies such as Microsoft make money by offering IT security services which are in reality a protection against Microsoft's own inability to secure its products from the beginning.\(^6\) If Microsoft really wanted tech companies to be a new Red Cross, as Brad Smith suggests in his blog post,\(^7\) it would mean that the companies' 'pro-profit model' must be reconsidered.

This brings me to the last player to be blamed for the ransomware incidents and for the generally inadequate IT security: the states. According to Brad Smith, states are running away from their responsibility by not having reached any agreement about a set of international guidelines that limit the exploitation of vulnerabilities in commercial IT systems and require states to cooperate with each other and with companies to enhance IT security. In addition, more and more independent voices within the IT technical environment are beginning to point out that states should take responsibility for regulating market failures that allow poorly programmed software to float freely around the market.\(^8\) Clearly, the states have not sufficiently invested in and implemented standards that provide guidelines for when a product is ready for the market. They have not – as is otherwise the case in many other areas, including the pharmaceutical and food sectors – invested in an authority that may investigate and expose unsafe products and businesses. Also, they have left the private sector in the driver's seat when it comes to basic research in e.g. artificial intelligence and machine learning which may seriously redefine and reinvent information technological security in the twenty-first century.

In this section, I have approached Smith's proposal for a digital Geneva Convention from a slightly wider angle and thus shown that it is biased to make the states and their intelligence services the scapegoat. I have also shown that it is insufficient to point to a solution that

---


7)  Smith, Brad (2017) (final note 1).

exclusively comprises states, their diplomats and international lawyers. However, this does not mean that transparency about legal guidelines for state behaviour in cyberspace is not desirable. International law theoretically provides predictability and tools to punish or 'shame' actors when they violate the adopted rules. That is good for both companies and governments seeking stability and status quo internationally.

But while clear legal framework is basically desirable, the idea of opening negotiations on a digital convention for state behaviour is inappropriate because it:

1) ignores the diplomatic difficulties caused by such opening
2) *de facto* undermines the potentials in the existing formal and informal talks about international law in cyberspace
3) does not take into account that the states' exploitation of IT vulnerabilities may also benefit their national security
4) overestimates the power of law in relation to the practical and technical enforcement challenges currently presented by cyberspace

In the following, I will take a closer look at these four items.

**Pandora’s Box**

The broad support for a digital Geneva Convention rests on an assumption (or perhaps a naive hope) that UN convention negotiations are merely a matter of states meeting and agreeing to the principles and rules that the US (or Microsoft) want to apply. This is obviously not how such diplomatic negotiations unfold, and in this particular case, the US, the EU countries and several like-minded nations have been actively fighting against the opening of a discussion on a new broad digital convention for several years. This group of 'allies' wants to adapt the behaviour of states in cyberspace to existing international framework, and the states have therefore negotiated separate resolutions on sub-elements of the digital area, such as human rights and privacy.

Thus, it follows from the logic of not biting off more than you can chew that the EU and the US – rather than a new convention – will try to get more and more countries to sign up to and further develop the already existing, though outdated Budapest Convention on cybercrime from 2001. This is first and foremost the case because the 'Western coalition' does not – as previously – have a majority in the UN and therefore cannot impose its own agenda. Opening negotiations on a new digital convention, which countries like Russia and China have been advocating for years, will mean a (re)opening of a number of issues that most Western countries do not want to discuss in an international forum. These issues are e.g. about control of the internet’s protocols (internet governance), which the West for years has struggled to regulate through cooperation with private parties, volunteers, non-profit organisations and companies and not through the UN. On the other hand, China and Russia will in all probability consider Smith's proposal about a digital Geneva Convention as a welcome opportunity to reopen the

In other words, diplomatic negotiations of this nature are slow and complex, and it is difficult to predict whether a proposal for a convention text will end with the desired outcome. This means that although Microsoft's recommended principles for online state behaviour would no doubt improve the IT security, a fully negotiated digital convention will not necessarily be beneficial to Microsoft and other IT companies (or the Western states in general). The convention negotiations may well result in increased state control of data that is currently in the hands of private companies and constitutes an important part of the companies’ current and future growth bases. Therefore, it cannot be ruled out that a majority of states in the UN will succeed in imposing a greater legal liability on companies, including liability for damages, when they develop malfunctioning software. This has previously been aired in international fora,\footnote{The UN General Assembly (2015a). “Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General” 69th session, agenda item 91. May be accessed at: http://undocs.org/A/69/723 (most recently accessed on 8 August 2017).} and it is something that US companies have been fighting, claiming that it would hurt the growth of the IT sector.\footnote{Goertzel, Karen M. (2016). “Legal Liability for Bad Software”. Crosstalk, September-October. May be accessed at: http://static1.1.sqspcdn.com/static/f/702523/27213494/1472233517737/201609-Goertzel.pdf?token=xi3hjI%2Btv66tqXCQp5LTh4veBQe%3D (most recently accessed on 8 August 2017).}

In this case, the slowness of major international negotiation processes could also mean that the technological development will constantly be overtaking the negotiations. The inertia makes it unlikely that the states will wish to finalise the various chapters on an ongoing basis, thereby relinquishing the possibility of developing the legal framework step-by-step. Consumers and businesses will therefore have to wait for many years for the states to reach agreement on all stipulations in a new convention.

**Existing Diplomatic Channels**

Smith recommends that states support the businesses in their efforts to secure their products, simultaneously limiting the development, storage and use of cyber weapons. This applies especially to weapons that make it possible to exploit companies' IT vulnerabilities. These recommendations, presented at the largest cybersecurity conference in the US, the RSA, and subsequently in a blog post,\footnote{Smith, Brad (2017) (final note 1).} are well in line with what has already been discussed (and will be discussed in the future) in several international fora. As opposed to a digital Geneva Convention, many of these fora are not legally binding, which is currently the only thing the
participating state and non-state actors have been able to agree on. This is the reason why several international legal and political experts continue to insist that non-binding declarations seem to be the most likely first step toward more solid national standards for cyberspace behaviour.13

The UN group of government experts within this field (UNGGE) has published reports on several occasions, showing that agreement has been reached on a number of related issues. However, despite the fact that the reports are non-binding, it has proved extremely difficult to agree on them. As an example, the latest round of negotiations in 2016/17 did not produce a new report at all. If non-binding reports cannot be negotiated, it is unlikely that a binding Geneva Convention is a viable option.

This does not mean though that UNGGE-like fora are not worth investing in. In previous UNGGE reports, the group of government experts agreed on the following: states acknowledge that existing international law applies in cyberspace, states do not deliberately harm other people's critical infrastructure or the units that states use to quell cyberattacks (CERTs), and – finally – states may not use proxies such as non-state actors to hurt others in cyberspace.14

In addition, the work among negotiation participants in both UNGGE and OSCE continues to create platforms for confidence-building measures. Such measures have historically acted as first steps, leading to serious talks on disarmament. All of these fully negotiated elements may have to start all over if all UN member states sit down to begin official negotiations on an overall digital convention.

Smith correctly points out that existing international law does not directly address – or significantly limit – states’ exploitation of the products of private IT companies when cyber weapons are being prepared or cyber espionage is carried out. The most comprehensive academic work attempting to clarify existing international law in cyberspace, the Tallinn Manual 2.0, emphasises that cyber espionage as such is not prohibited unless it results in functional harm, violates international human rights etc.15 Although the Manual has been prepared by academics, it has already in several countries become a central reference document

Prioritising Denmark’s Cyber Policy

for state employees who need to clarify and legally evaluate the respective states’ military use of cyberspace.

If Microsoft is to pin its hopes on the addition of a chapter on a ban on state exploitation of IT vulnerabilities in private companies, this should be formulated more precisely and focused than as a broad need for a digital Geneva Convention. In this regard, Microsoft is getting more out of quietly continuing its work to influence the states that are engaged in ongoing negotiations in e.g. UNGGE and work to ensure that the agreed recommendations are converted into binding international practices.

Even if Microsoft succeeds in getting a voice in these negotiation fora, it is highly unlikely that the states are willing to be legally obligated and thereby completely give up the right to develop, store and use cyber weapons. I will point out two reasons for this.

Conflicting Security Concerns

There is a good explanation as to why espionage as a rule does not violate international law. In the attempt to predict and prevent wars, terrorism and crime and to strengthen international negotiation positions, espionage has always been a valued tool for states. With the prevalence and dependence on information and communication technology, states have obtained a platform where retrieval of large amounts of information has become easier and almost risk-free. Skilled hackers in the intelligence services are able to sit in peace and quiet in their home country and look for and exploit the IT vulnerabilities of adversaries.

The source of Microsoft’s significant intervention derives from the well-known cyberspace dilemma: that many of the identified and exploited IT vulnerabilities are found in commercial IT products used by state institutions, companies and private citizens all over the globe. The dilemma occurs as soon as a vulnerability has been identified in a system. In that moment, an intelligence service must necessarily evaluate which IT systems are exposed due to the IT vulnerability, both in its home country and with its allies, and what other actors are aware of it, will be aware of it and are currently exploiting it. Such evaluations may be extremely difficult.

However, state exploitation of IT vulnerabilities may also increase the national security. This recognition of the opposite security considerations is what led the US to develop an official (although classified) procedure for assessing whether the potential benefits of exploiting an IT vulnerability measures up to the potential risks associated with the fact that the vulnerability is not being corrected by the company behind it.

If you are a supporter of Microsoft’s agenda on less state cyberspace armament, it might be more important to start with something other than a convention on state behaviour in cyberspace and instead seek more openness regarding the foundation for the various states’ evaluations of IT vulnerabilities. In addition, supporters must necessarily try to convince both the public and the politicians that global IT security is an important part of our 'national security', even if it
complicates the work of police and intelligence services. In other words, support must develop strong arguments as to why IT security is more important than the ability (via cyberspace) to dominate in future military confrontations or have knowledge about other states’ unofficial positions and attitudes regarding important international economic and diplomatic issues. Thus, Microsoft and other supporters of a digital convention would have to seriously engage in and confront the existing dilemma rather than ignoring its existence.

Even if various tech giants and their supporters are successful in setting up a story that IT security needs to have a higher priority at the expense of other types of security, the decision to give up the ability to exploit vulnerabilities in cyberspace is still difficult. This is due to a number of technical factors.

**Enforcement Problematics**

As mentioned above, in 2015 UNGGE reached agreement that states may not use proxies to harm each other. Besides, there are already clear guidelines to which states may diplomatically refer if e.g. another state interferes in a democratic electoral process, like the US believes Russia did in 2016. Granted, the UNGGE conclusions are not yet legally binding which may be the reason why some states seem willing to ignore them. However, it is far from certain that the legal word (in cyberspace) would be as strong as Brad Smith hopes. The technical nature of cyberspace makes it difficult to enforce a convention.

It is an often repeated basic assumption about the technical nature of cyberspace that it is relatively easy to remain anonymous. Most online crime is not solved, and the people being WannaCry or NotPetya have not yet been apprehended. When a major cyber incident takes place, the injured state often accuses another state of standing behind it – and just as often the accused state rejects the accusation. However, this does not prevent the injured state from taking action against the presumed state culprit. As an example, the US threatened China with sanctions for industrial cyber espionage which the US believed it could trace back to the Chinese state, and the US expelled 35 Russian diplomats after all US intelligence services had pointed to the Kremlin as responsible for the hacker attacks on the democratic presidential campaign. However, it is not clear which technical evidence the US is using as the basis for identifying the wirepuller. This is primarily due to the lack of US interest in losing the collection capacity which the country possesses. If you reveal the evidence, the signatures and the techniques which you know the counterpart is using, the counterpart is likely to change its practices in the future. In relation to the burden of proof and thus the enforcement of possible international rules, this dilemma is a key challenge in any negotiation on a digital convention.

Inspired by the International Atomic Energy Agency (IAEA), Brad Smith proposes to establish a group of independent technical experts who shall determine whether a cyberattack is the
work of a state actor. The idea is certainly interesting and worth considering, but it is also potentially controversial. This is due to the fact that it seems unimaginable that some states would be willing to let participants from such international agency physically monitor the work of their intelligence services in cyberspace. Without physical surveillance, the agency would in fact act in the same way as cybersecurity companies, such as CrowdStrike, Kaspersky and FireEye, which already today thoroughly analyse the instances of illegal intrusion that take place in cyberspace. In spite of the great technical skills of these companies, it is far from certain that they have the ability to sufficiently lift the burden of proof against a state that is careful to remain anonymous. An intelligence service with extensive surveillance capabilities which also uses cyber espionage itself and maybe even informants on the ground would no doubt be able to do it. But nobody would probably be willing to let an international cyber watchdog act as a *de facto* United Nations espionage agency.

International ‘shaming’ in connection with breach of conventions has sometimes proven to be a useful tool in international diplomatic contexts, but it requires attribution. Unless you technically want to caulk the internet, an international cyber agency will lack factual espionage authority, but with a mandate to investigate cyberattacks, it is currently the most probable, concrete bid for something that in time might be agreed on and which might even be the starting point for further negotiations.

**Denmark’s Political Latitude**

Above, I have pointed out four reasons why efforts to establish a convention for state behaviour in cyberspace are doomed to fail. However, this does not necessarily mean that the extent of cybercrime and other cyber incidents will continue to increase forever. A number of evolutions may be able to remedy the problem. Firstly, there is still hope that the technological development will be able to improve IT products and their implementation. Secondly, it cannot be ruled out that non-binding diplomatic negotiations over time may actually create standards that lead to less state collection and attack activity in cyberspace. Thirdly, especially the US, but also China and the EU, hold a possible key to enhancing the general IT security through regulations, standards and new incentive structures. This raises the question: What can the Danish government do to pursue Denmark’s interests in this area? In the following section, I have three suggestions for efforts that Denmark should prioritise. These could very well be included in the coming Danish cyber strategy.

**Cyber Diplomacy**

So far, Denmark has not asserted itself within the cyber diplomatic field to any great extent. Unlike our Nordic neighbours which all have a cyber ambassador, the appointment of a Danish technical ambassador in Silicon Valley bears witness to the fact that Denmark’s priority is not diplomatic negotiations on standards for state behaviour in cyberspace or protection of human rights online, but rather growth stimulation in the IT sector. In other words, Denmark
has decided to trust that other countries will defend Danish interests with respect to e.g. the question of state behaviour in cyberspace. If the Danish government wishes to influence what is going to happen in the area, the Ministry of Foreign Affairs must necessarily be given financial means so that Denmark's tech ambassador – whose main focus is financial growth – is supported and receives input from a number of employees, e.g.:

1. An EU cyber attaché in Brussels who would be able to leave a mark on the cyber diplomatic game in the EU, which is still taking shape.
2. An employee, for example, at the UN mission in New York with the specific goal of getting a Danish expert and diplomats admitted to future UNGGE-like cyber norm promotion initiatives.
3. An interdisciplinary team at the Ministry of Foreign Affairs in the legal, security and trade policy departments, e.g. anchored under the political director, with responsibility and liberty to develop and coordinate the legal and security policy line within the area.

**Better Regulation of the IT Sector**

Recent Danish governments have not taken any initiative to invest in the development of regulations and standards for the Danish market for IT products. Fundamentally, it is a challenge for a small state like Denmark that there are not many opportunities to make demands on and regulate large multinational IT companies. However, at a time when the need for state intervention in the IT product market becomes increasingly clear, the Danish government, together with the other EU countries, has a responsibility for setting up a clear framework that the companies need to comply with. In the US, which is generally reticent with any kind of regulation, the White House's Commission on Enhancing National Cybersecurity, featuring senior US business participants, presented a report in December 2016. The report's authors recommend more IT security standards and – if these are not followed – regulation. A similar development should also take place in the EU. The sooner the Danish Business Authority and the Ministry of Industry, Business and Financial Affairs acknowledge the need for regulation, the sooner they can develop useful standards as well as licensing, penalty and incentive schemes in cooperation with Danish companies. It would also make Denmark a policy maker (and not just a ‘policyholder’) in the EU, which ultimately would give Danish companies a competitive edge. A concrete recommendation proposed by the White House’s Commission on Enhancing National Cybersecurity is e.g. the development of a ‘rating system’ for the security of commercial IT products.17

---

Prioritising Denmark’s Cyber Policy

A Stronger Cyber Protection

The Danish defence has received funds for both the use of cyberspace to retrieve data and as part of future military operations. As mentioned above, these activities often present a dilemma. The vulnerabilities of enemy IT systems that are exploited sometimes stem from commercial IT products, which are used in Denmark and in the rest of the world. Like the US, the Danish defence should develop procedures for storage of such vulnerabilities and when and how they are shared for remediation. Such procedures should balance the consideration for IT security with the need for collection to protect Denmark’s security. Clear standards and demands on companies that develop, sell or implement IT products may help the defence make the right decisions.

In addition, a procedure for IT vulnerability assessment should be added to the agenda and discussed with Denmark’s allies in NATO in order to establish common guidelines. It is not in Denmark's interest that our allies develop military capabilities without regard to the consequences which the use of IT vulnerabilities might have across the alliance. Proposals for common guidelines and concrete initiatives for cooperation are usually first developed in academic and non-state fora. Therefore, it would be an advantage for the Ministry of Defence to apply for membership of and sending a cyber policy worker to the NATO Cooperative Cyber Defence Center of Excellence in Tallinn.

Conclusion

Microsoft’s proposal for a digital Geneva Convention is an attractive idea: Clear legal guidelines which restrict state cyber armament and cyberattacks on critical infrastructure and a deeper state cooperation with the technology industry to identify and remedy vulnerabilities are important measures. In this brief I have, however, presented a number of arguments as to why the opening of negotiations on a convention on state behaviour in cyberspace is not the right path to follow. If you want to increase the overall IT security and thereby minimise the risk of ransomware, Denmark should rather prioritise a series of other efforts.

Smith’s Digital Geneva Convention implicitly builds on the assumption that it is only the state and its intelligence service that is the problem in cyberspace and that the solution is primarily an international legal issue. However, states are far from the only players with responsibility for solving cyberspace challenges. The affected companies that have not adequately complied with basic IT hygiene are left out of the story. Left out are also the technology companies who – in their eagerness to enter the market quickly (rather than safely) – have produced defective software. This means that a digital convention, if it is actually finalised, will formally define the legal limits for state intelligence and military activities in cyberspace, but it will not address the fundamental vulnerabilities that today exist in cyberspace and which continue to be developed by the companies.
Having said that, it is unlikely that a digital convention in the form recommended by Microsoft can be finalised even though Denmark, the EU and the US might be well-disposed toward such convention. This is due to the following:

1) That the opening of a negotiation process under the auspices of the UN is likely to lead to diplomatic discussions on issues that Denmark and Denmark’s allies do not want to reopen in a large-scale digital UN convention. This could e.g. be about the governance of the internet protocols as well as freedom of expression and other fundamental human rights online.

2) That a negotiation process may undermine the existing formal and informal discussions on international law in cyberspace. The guidelines which states have agreed on in e.g. the UN Group of Government Experts (UNGGE), the confidence-building negotiations that states have slowly sought to restore in the OSCE, and the indirect influence on government work offered by research in international law, e.g. the Tallinn Manual 2.0., risk having to start over with the opening of negotiations on a digital convention.

3) That States exploit IT vulnerabilities to capture criminals, prevent terrorism and predict military confrontations just like they exploit IT vulnerabilities to improve their negotiating position in international negotiations. It is unlikely that states will abandon these prerogatives.

4) That a convention on state behaviour in cyberspace is difficult to enforce. States are rarely willing to reveal the technical evidence they possess as this would prevent future collection. As Brad Smith points out, one solution is an international cyber agency which would monitor and investigate cyber incidents. Although such agency never gets access to state intelligence services, it is a concrete recommendation that might be a better starting point for international negotiations than an all-encompassing digital convention.

The fact that a convention has long and not necessarily very optimistic prospects does not mean that Denmark should just lean back in the cyber political and cyber diplomatic field. Cyberspace has come to stay, and if Denmark wants to influence the rules that will inevitably regulate the behaviour of states and companies within the digital field, the current government must invest more resources to keep abreast of the development. In concrete terms, this implies the following:

a) That the Ministry of Foreign Affairs should be given means to increase its cyber engagement in the EU, the UN and in the Ministry itself which may support the newly appointed tech ambassador from a cybersecurity policy perspective.

b) That the Ministry of Industry, Business and Financial Affairs should as soon as possible recognise the need for regulation and set up cooperation with Danish companies on developing standards as well as licensing, penalty and incentive schemes.

c) That the Ministry of Defence should develop a procedure that clarifies when vulnerabilities are stored and when and how they are shared with a view to remediation. These thoughts should be brought along to NATO, as it is not in Denmark’s interest that allies develop military capabilities without taking the general IT security of NATO’s member states into account.