2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011 © CCD COE Publications

Is the Swedish Territorial Defence Ordinance applicable on the fourth arena?

Victoria Ekstedt
Legal adviser at the CNO Unit, Swedish Armed Forces
Enköping, Sweden
victoria.ekstedt@mil.se

Abstract- **Like other modern societies, Sweden is highly dependent on its digital infrastructure in order to run vital functions such as electricity, water purification, information and communications. Even though this infrastructure is characterized by transboundary features, it is clearly a part of the Swedish state. In peacetime, the Swedish armed forces are tasked to protect and defend the geographic territory of the state from violations, and the authority to do so is given by the Territorial Defence Ordinance. However, according to the analysis of this paper, the ordinance can not be applied on the digital parts of the society, by the military called "the fourth arena". Numerous difficulties rises with an application of the ordinance in its present wording and against this background, it is of interest to clarify the present legal situation and suggest a way forward in order to achieve adequate protection on the same premises as the other arenas. The interdependency between national and international law on this matter is pointed out and international law is used to interpret the national ordinance. The conclusion is that the Swedish politicians and legislators' needs to find legal support for the defence of the Swedish digital interests and infrastructure by seeking cooperation and legislative solutions in an international context and by doing so, hopefully the national legislation will follow. The legal challenges faced by Sweden are likely to be similar in several comparable countries, why this discussion should be of interest for other states and held in an international context.**

Keywords: digital territory, international law, violation, transboundary features

I. INTRODUCTION

The Swedish armed forces are tasked by the Swedish government to defend and protect the territorial integrity and national independence of Sweden in accordance with international [1] and national law [2-3].
The Swedish Territorial Defence Ordinance (the ordinance) [4] is the national legislation which authorizes the armed forces to defend the Swedish geographic territory in peacetime, at least regarding the three traditional military arenas (land, sea and air). Most states have national legislations with similar function to the ordinance since in a society founded on the rule of law, the authority for state officials to use force have to be expressly given and regulated by law in order to fulfill the requirements of legality and human rights . The ordinance is the national interpretation and implementation of the international law principles on state sovereignty and the right not to have its territory violated by other states [5]. It gives the armed forces the right and duty to defend the territory by using force if necessary, during *jus ad bellum*, the lawful resort to force in peacetime. In case of a war situation, *jus in bellum*, the ordinance ceases to apply and will be replaced by the Laws of Armed Conflict, LOAC [6]. It is undisputable that the armed forces are obliged to defend the Swedish digital infrastructure in case Sweden becomes involved in a war on the same legal prerequisites, *jus in bellum*, as the other arenas. Equally clear is that if a computer network attack is to be regarded as an "armed attack" in accordance with article 51 of the UN Charter, this would constitute a right to self defense in the same way as the other arenas. However, the threshold of an "armed attack" in a digital context is yet to be defined [7] and from international state praxis, we can conclude that no computer network attack have yet been categorized as an "armed attack" according to article 51. In addition, the difficulties to identify the perpetrators and/or the responsible state in conjunction with a strong political context have an aggravating effect on the development of praxis on this legal area.[1] This directs our main focus to peacetime incidents and conflicts, where the territorial ordinance is applicable, and not in the context of war or an armed attack. The question about the definition of a "digital territory" is however equally important both in a *jus ad bellum* as well as in a *jus in bellum* context.

The international legal framework from where the territorial ordinance origins were developed in an era when the digital revolution were yet to be born. The technical development and the information revolution bring with it an entirely new set of requirements which stretches beyond the existing legal labels and structure. To be able to deal with the digital dimension, the international legal framework have to be prepared to develop to avoid the risk of becoming outdated or end up being contra productive and thereby short-circuit itself. Swedish (and most other) military doctrine

1 For example, the attack on Estonia in 2007 were initially regarded as an article 51 attack by a statement by the Estonian Prime Minister Andrus Ansip, but it was later withdrawn by the Minister of Defence Jaak Aaviksoo after discussions with EU and NATO since NATO at that time did not consider cyber attacks as a clear, military action.

is more easily developed than laws, and embraces the fourth arena which is the same thing as we in daily language call the digital infrastructure of the society but in a military context. Computers, Internet, networks and other sorts of data form an integral part of our society and its importance as well as our dependence of it is steadily increasing [8]. The Swedish government and the Ministry of Defense are fully aware of this development, which becomes clear in the latest bill " A functional defense" [9]. The bill points out the increasing importance of the digital infrastructure and that the threats against it have risen. The risk of a full scale cyber war taking place is not regarded as the most plausible or imminent threat, instead focus is set on the risk for cyber incidents and conflicts of a lesser magnitude, including web based criminality. Today, there are numerous international examples of cyber incidents and conflicts, from large-scale computer network attacks such as those which took place in Estonia 2007 and in Georgia 2008, to the Stuxnet virus in 2010 [10] and computer network exploitations such as secret intrusions, espionage and numerous thefts of information which happened to Google in China [11] and the US Defense in 2010 [12] . NATO and EU circulated warnings to protect secret intelligence material due to cyber attacks originating from China, and it was concluded that the EU system was vulnerable due to the fact that security efforts were the responsibility for each member state [13]. The Swedish foreign minister Carl Bildt has emphasized in the Statement of Government Policy 2010 as well as in articles in national and international press [14] the need to acknowledge the importance of the threats against the digital infrastructure and the Internet. He underlines the importance to protect the freedom of speech and the need for enhancement of the security on the global digital arena, not necessarily by regulating the Internet but by finding ways of discouraging the perpetrators. Finally, the Swedish EU Commissioner Cecilia Malmström points out the importance for states to cooperate in order to effectively handle the transboundary nature of digital threats. She is presently working active to strengthen the capability within EU [15] as well as initiating a dialogue with NATO and the United States.

Against this background, it is of interest to clarify whether it is possible for the Swedish armed forces to apply the ordinance on the fourth arena in order to protect the digital parts of the society in peacetime, *jus ad bellum*. The conclusion is however highly doubtful and the Swedish politicians and legislators needs to find a solution to this dilemma.

II. THE TERRITORIAL DEFENCE ORDINANCE

According to the Swedish Territorial Access Ordinance [16], foreign state owned vessels and vehicles need to get an advance permission to enter Swedish territory except from emergency situations or for innocent passage.[2] The Territorial Defence Ordinance becomes applicable when a state owned subject violates these rules in any

2 The expression "innocent passage" means that vessels by sea may pass through the territory under certain circumstances, for example without any stops, passing at a certain distance from the Swedish territorial waters and such. This rule has its origin in the UNCLOS, United Nations Convention on the law of the Sea article 17-19.

way. An unauthorized presence on Swedish territory gives Swedish armed forces the right and duty to react, if necessary by using force.

III. A NATIONAL DIGITAL TERRITORY?

The geographic territorial borders of Sweden can be determined by treaties, conventions, maps and nautical charts. However, there is no definition on where the ”digital borders” are drawn. If we can not determine a territory, it will be equally difficult to say whether an infringement has taken place or not. Therefore, a prerequisite to apply the ordinance on the fourth arena is to have some sort of territory and borders defined. This in turn implies that the legislation can not be applied in its present wording due to the unique and significant circumstances the digital dimension carries with itself. It is to some extent possible to define a digital territory on the same conditions as for the geographic territory since the digital infrastructure has geographic connections such as wires and cables, servers, nods and the software used on these. The hard- and software which keep up the digital infrastructure of a state could in this sense constitute a Swedish digital territory where information can be created, stored and pass through. Unfortunately, this suggestion is associated with several problems. For example, state owned information is not always handled within the geographic borders of Sweden. A recent investigation [17] showed that almost twenty percent of the Swedish authorities and municipalities were at risk at having their e-mail bugged due to the fact that their spam filters were located in foreign countries by “cloud computing”. If information for example should be stored at a server in another country it is highly questionable whether it is defendable at all, at least by Swedish armed forces. But how important is it to talk about borders and territory in this context when the digital dimension care so little about geography? Well, since the legal framework can not simply abandon its present structure, it have to continue to be fastidious about borders and national territories and this in turn, means the need for a solution to the problem remains.

IV. PRINCIPLE PROBLEMS

The ordinance primarily deals with the presence of state subjects and not of individuals. A consequence with an application of this ordinance on a digital territory is that every subject that wants to access the Swedish digital territory would have to be identified and classified as a state subject or an individual in order to initiate the process of giving permission to enter or not. Of course, this is an impossible task to perform and it is against several principles. In addition, according to the international law principle on proportionality the actions taken by a state to protect and defend its territory are not unlimited; they have to be proportionate to the violation. It is doubtful whether such procedures would be acceptable according to this principle. Finally, the founding idea of the Internet that information should be free and accessible for everyone would be violated, and the extensive surveillance would be against several human right principles, such as freedom of speech and the right to privacy [18].

V. LEGAL PROBLEMS

The alternative to adjust the ordinance with the purpose of facilitate its applicability on the fourth arena is problematic due to the fact that this law origins from the international law regarding state sovereignty and the right for states not to have their territories violated by other states [19]. International law is not possible to change for a single state, but states can refine and develop it by interpretation and then make own political standpoints. There are numerous examples when states declare their opinion of the law in specific cases, for example Russia has declared that they equal computer network attacks with the use of weapons of mass destruction [20]. An adjustment of the ordinance to the special conditions of the fourth arena has to have a strong connection to the political official standpoint with regard to international law, and as long as this is not developed on the digital area, neither will the ordinance.

The ordinance is only applicable on violations in peacetime, *jus ad bellum*, which means it does not embrace violations which amount to an armed attack on Swedish territory, *jus in bellum* [21]. If the ordinance is to be used in its present wording, it is necessary to define the expression "violation" in a digital context. Comparing what would constitute a "violation" on the other military arenas, the ordinance would regard the mere unauthorized presence of a foreign state subject on Swedish territory as a violation. Using a strict interpretation in the digital context, a violation would be any foreign state actors' presence on the Swedish digital territory, for example entering a Swedish website without some sort of an advanced permission. Even if such analogy is well in line with the wording of the regulation, this is obviously not going to be practiced. However, if we choose to take a step away from the strict legal wording and interpret violation as something more intrusive than the mere unauthorized presence, "violation" would mean intrusions in digital areas not open for public access. Such intrusions with the purpose of gaining access to areas which contains data otherwise restricted in order to achieve information or to be able to navigate in otherwise closed networks, means we end up in a completely different set of laws. Still and only due to their digital features, these cases will not be handled by the ordinance or the Swedish armed forces, but by the Swedish police. These actions are primarily categorized as criminal acts and they are sorted legally under national criminal laws. However, at the same time, they are equally infringements of article 2.4 UN Charter if committed by a state. Digital intrusions could also be regarded as a use of force [22] in this sense, however not particularly serious due to the lack of the element of being "armed", i.e. no weapons are used, or because their effects are not severe enough [7]. In an EU context, these intrusions are also illegal actions according to the Council Framework Decision on attacks against information systems and the Council Framework Decision on combating terrorism [23].

Another complicating factor is that in case of a violation of a Swedish digital asset which is geographically situated outside the Swedish territory, neither the Swedish police, nor the Swedish armed forces have any right to protect or defend it. In these cases, the only alternative is to be reliant on the actions of the authorities of the

country where the asset is placed. Another feature, however equally difficult, is the situation of interdependency between states, i.e. when a state is dependent on the function of digital assets and infrastructures owned by another state. Sweden is for example operating one of the thirteen root servers in the world which provides the key element of the domain name infrastructure of the Internet. Operating the root server and keep it stable and secure is certainly of interest for other countries than Sweden, even though they have no jurisdiction to take actions in case needed [24].

VI. PRACTICAL PROBLEMS

Why not solve the problem by claiming a Swedish digital territory and then apply the ordinance on the fourth arena in its present wording? The argument to do so is simple – why should not general rules be applied on the digital parts of the society as well, especially with regard to its increasing importance. Unfortunately, this solution is too elementary due to the far reaching consequences it would bring and as we must take into consideration. For example, it would demand that the digital borders would have to be constantly monitored and that, taking into consideration the amount of traffic passing these borders every day would be an extensive on the verge of impossible, task to perform. Further on, the definition of the border would need constant and immediate updates since it would be defined by the existence and use of hard- and software within the geographical Swedish territory and that development is a constant and uncontrollable process. However, there is digital infrastructure which is indisputably placed within the geographic borders, and thereby could constitute at least some parts of a Swedish digital territory. Unfortunately, the crucial information needed in order to apply the ordinance is where the border of the digital territory is. This means that even if information on the digital geography is provided in part, it will be impossible to draw a complete borderline and defend it in the same way the other arenas are doing. If the borderline can not be drawn, there is also a risk that the society will have different levels of protection, or in worst case, not be defended at all, which is a problem. Due to this, an application of the ordinance in its present wording on a Swedish "digital territory" does not appear to be practically possible at all.

In summary, there are principal, legal and practical problems which speak against an application of the ordinance on the fourth arena. To make use of this ordinance on an arena where completely different standards and conditions prevails implies a number of undesirable consequences.

VII. ARE WE GOING TO PROTECT AND DEFEND SWEDEN INCLUDING ITS DIGITAL DIMENSION?

If the ordinance cannot be altered to fit or be applied onto the fourth arena, and no digital borders are possible to draw, does this mean the Swedish digital society shall not be protected and defended as the land, air and sea territories are against violations? Is this a fair consequence of having an inadequate regulation? The answer to this question is without hesitation that the whole society shall be protected and defended,

including its digital parts. This intention is clearly proclaimed by the politicians in the latest defence bill [25] issued by the government. The content of the bill is one step in a direction towards a possible solution by discussing the tasks for the Swedish armed forces as well as national security, sovereignty and independence in a global context. By pointing out threats as well as their solutions as something which no longer necessarily occurs or is to be protected and defended within the national borders, but in our immediate region and beyond, the government stretches the Swedish responsibility beyond the geographic territory. The ratification of the Treaty of Lisbon, the article 47.2 of the Treaty of the European Union (TEU) and the solidarity clause in the Treaty on the Functioning of the European Union (TFEU) article 222 strengthens this view and implicates that Sweden is prepared to comprehend and take responsibility for the security for at least the other member states of the EU. This view was also established by the "solidarity declaration" made by the Swedish parliament in June 2009 which states that Sweden will not be passive in case a catastrophe or an attack would occur in another EU member state or a Nordic country. This declaration covers both civilian as well as military crisis which is an advantage in a digital context, for example with regard to the problem of identifying the perpetrator. However, the prerequisites for such cooperation are still to be developed and since the specific purpose of the ordinance is to give the Swedish armed forces the authority to defend the Swedish territory, the applicability of the regulation is strictly national and will not provide adequate legal basis for such cooperation.

VIII. LEGISLATION AND/OR INTERNATIONAL COOPERATION – A WAY FORWARD?

A possible legal solution to the problem is to write a new and separate law, which defines what parts of the digital society to be considered as critical for its function and provide the Swedish armed forces with authority, strictly restricted to these parts, to defend it from violations in peacetime. There is already a law [26] which gives this authority to Swedish armed forces to guard specific objects and buildings as they consider need to be protected from unauthorized access by the public in order to prevent sabotage, terrorist actions and espionage, but it do not apply to the digital infrastructure. Creating a similar regulation for digital infrastructure which needs to be protected could be a way forward in order to ensure the function of the society and at the same time take international responsibility in order to strengthen the global digital security. Although, this is only a half-way solution since it will not be the same as defending the whole digital infrastructure of Sweden. It will only strengthen the protection of parts of the infrastructure in case of violations. In addition, the political history of Sweden makes it difficult for politicians to legislate against a strong public opinion that the armed forces should not be put at risk of using force against citizens on Swedish territory.[3] Due to this reason, the chances of having this type of legislation are highly uncertain. Another suggestion which already has been addressed is to put

3 The strict division of tasks between the armed forces and the police can be traced back to events that took place in Ådalen in 1931 where Swedish military fired at and killed 5 people at a demonstration.

the territorial questions aside and focus on efforts to strengthen international cooperation on these matters. One tool could be the development of the content of the solidarity clauses in the TEU and the TFEU. Additionally, with increasing interoperability and interdependency between countries, there should also be of interest to discuss if there are duties countries would owe to each other in protecting their digital infrastructure; however that question is too large to be addressed further in this paper.

IX. CONCLUSIONS

In summary, we can conclude that the ordinance can not be applied on the fourth arena due to principal, legal and practical problems. At the same time, there is a clear intention from the political leadership that the Swedish digital infrastructure shall be protected and defended. All modern societies are highly dependent on the function of their computers, networks and communications, which is a strong indicator that this ambition will not change. The unavoidable conclusion is that if the ordinance cannot provide a legal basis for the protection and defense of the Swedish digital infrastructure in peacetime, the legislators have to find a new solution, especially taking into account that the fourth arena operates under special circumstances, not always easily compared with the other parts of the society. Efforts have already been made by the politicians in creating security in a global context and this should continue to be a highly prioritized goal. If an international system of cooperation is established with the purpose to better protect the digital assets of states and a legal position has been worked out to ensure its function, less attention will be drawn to geographical territory issues, and surely national legislation will follow in order to meet the needs of the twenty first century instead of trying to adjust the features of the modern society to an outdated legal order.

REFERENCES

[1] Charter of the United Nations (1945). Available at http://www.un.org/en/documents/charter/index.shtml

[2] Swedish Constitution, Instrument of Government (1974:152) 10:9

[3] Ordinance with Instructions for the Armed Forces (2007:1266) §2

[4] Territorial Defence Ordinance, in full English translation the ”Ordinance (1982:756) concerning intervention by Swedish Armed Forces in the event of violations of Swedish territory in peacetime and in neutrality” in Swedish. “Förordning (1982:756) om Försvarsmaktens ingripande vid kränkningar av Sveriges territorium under fred och neutralitet, mm.”

[5] UN Charter (1945) article 2.1 on state sovereignty and 2.4 the principle about non-intervention between states, The UN General Assembly resolution 2625 (XXV) the “Declaration on Friendly Relations” (1970) and international customary law principles.

[6] The humanitarian laws (Geneva Conventions (1949) I-IV and Additional Protocol (1977) I and II), laws on Neutrality (Hague Conventions (1907) V and XII) and law on Occupation (Hague Convention (1907) IV)

[7] T. Wingfield, “When Is a Cyber Attack an" Armed Attack?": Legal Thresholds for Distinguishing Military Activities in Cyberspace,” *Potomac Institute for Policy Studies*, 2006.

[8] A thorough picture of our dependency of the Internet is given in the Council of Europe Secretariat report ”Internet governance and critical Internet resources” p.7-29 (2009)

[9] The bill ”A functional defence”, Ett användbart försvar” 08/09:140 p. 28

[10] N. Falliere, L.O. Murchu, and E. Chien, “W32. Stuxnet Dossier”, *Symantech Security Response*, vol. 3, 2010, pp. 1-64. Available at http://www.symantech.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[11] Available at http://googleblog.blogspot.com/2010/01new-approach-to-china.html

[12] Statement by the Director of the US National Intelligence, Dennis Blair at the annual threat assessment at the US Senate 2010.

[13] Evans, Michael, “Cyberwar declared as China hunts for the West´s intelligence secrets”, *the Times* March 8 (2010)

[14] Swedish Foreign Minister Carl Bildt “Tear down these walls against Internet freedom” in *Washington Post* January 25 2010

[15] “Commission to boost EU´s defence against cyber attacks” Directive IP/10/12/39. Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1239

[16] Territorial Access Ordinance, Tillträdesförordningen (1992:118)

[17] Alert from the Swedish Fortifications Agency and Symantech “Myndighet slår larm om it-läckor” in *SvD* 2 february 2011

[18] European Convention of Human Rights (1950), articles 8 and 10. Available at: http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp

[19] UN Charter (1945) article 2.1 on state sovereignty and 2.4 the principle about non-intervention between states, The UN General Assembly resolution 2625 (XXV) the “Declaration on Friendly Relations” (1970) and international customary law principles.

[20] V.I. Tsymbal, “Kontseptsiya Informatsionnoi Voiny” (concept of information warfare) speech at RUS and US conference in Moscow 1995. For a complete overview see Swedish Defence Agency report “Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations” March 2010 on the Russian view on these topics.

[21] Ordinance (1982:756) concerning intervention by Swedish Armed Forces in the event of violations of Swedish territory in peacetime and in neutrality 1§

[22] For a general definition of the expression “use of force”, see UN General Assembly resolution 3314 “Definition of Aggression”

[23] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism and Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

[24] Council of Europe report “Internet Governance and critical Internet resources” p.9 (2009)

[25] The bill ”A functional defence” 08/09:140 pp. 8, 34-37

[26] Law on Protection, Skyddslagen (2010:305) (*authors´ translation*)