A Non-Attribution-Dilemma and its Impact on Legal Regulation of Cyberwar

Michael Niekamp
Institute of Philosophy
University of Osnabrueck
Osnabrueck, Germany
mniekamp@uni-osnabrueck.de

Florian Grunert
Institute of Philosophy
University of Osnabrueck
Osnabrueck, Germany
fgrunert@uni-osnabrueck.de

Abstract: The potential impossibility of attribution in cyberspace causes at least three challenges for international politics. This paper analyses the systematic role of the non-attribution-problem with regard to the definition of cyberwar, its impact on legal regulation and the strategy of 'deterrence through a threat of retaliation'. Firstly we provide a conceptual specification of non-attribution. Secondly, referring to a classical definition of war and a sound principle of self-defense, we provide a logical clarification of these terms for cases of non-attribution and their impact to define and classify 'cyberwar'. Afterwards we argue that any attempt to rational legal regulation under non-attribution will lead into a serious dilemma, which consists either in a *reductio ad absurdum* of the category of war and the impossibility of a sound principle of self-defense or the indistinguishability of a state of regulation and anarchy. However, the existence of this non-attribution-problem has no impact on the possibility of rational 'deterrence through a threat of retaliation', which in turn might lead to a complete prudential dilemma.

Keywords: cyberwar; deterrence; non-attribution-dilemma; legal regulation; logical clarification; deterrence

1. INTRODUCTION[1]

The potential impossibility of attribution in cyberspace causes at least three challenges for the international politics and its quest of 'cyberwar'. All three challenges are closely interlinked and we would like to reveal its connection. This paper analyses the systematic role of the non-attribution-problem with regard to the i) definition and classification of 'cyberwar', ii) its legal regulation and iii) the common strategy of 'deterrence through a threat of retaliation'.

A first challenge of 'cyberwar' lies in the field of its definition and our classificatory practice to subsume a phenomenon under this category. Some protagonist in the debate hold the opinion that there is no and there will be no 'cyberwar' in the sense of international law for *classificatory reasons* (e.g. Ziolkowski (2012), Kosina (2012), from a more technical perspective Lindner (2012)). They argue that we *should not* talk about 'cyberwar' unless there is a phenomenon that deserves such a classification, for example, when a sovereign state declares war (only) in cyberspace ('fifth domain'). They suggest that all current phenomena *should* only be treated as special cases of different types of conflict and should be labelled accordingly.

Although we partially agree on their point, we think that this is only the second best way to acknowledge what is really at stake here.[2] The impossibility of non-attribution make things even worse, because it causes a conceptual and not merely a classificatory problem. By providing a different approach and new line of reasoning, we draw the conclusion that under the condition of non-attribution we *cannot* talk about 'cyberwar' given our conceptual practice and usage of 'war'. If you nevertheless want to talk about 'cyberwar' you will have to change not only the classificatory practice, but more fundamentally the meaning of 'war'.

A second challenge of 'cyberwar' lies in the field of its rational 'legal regulation'. The most optimistic view emphasizes that our international law and its underlying standards are sufficient (in principle and de facto) to solve all emerging problems even under conditions of non-attribution (e.g. Heintschel von Heinegg (2011) quoted in ['left blank intentionally'] (2012); Hoyer (2011)). The most sceptical view is presented by Gaycken (2011,69; our translation), who postulates "the impossibility of global regulation". Although we lean towards a sceptical view, we'll provide a totally different and more consistent line of reasoning for the impossibility of a rational legal regulation by formulating a non-attribution-dilemma.

---

[1] We would like to thank the participants of the 'DeepSec Conference 2012' and three anonymus reviewer of the CCDCOE for helpful comments on a previous version of this paper. In particular we are grateful to Nikola Kompa, Rudi Müllan and Julian Kröger for very helpful discussions. Needless to say that possible typos and idiosyncratic phrases remain to our responsibility.

[2] As Hayden (2011,3) phrases it in the context of the whole 'cyber'-thing: "Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon."

A third closely related challenge regards the question whether 'deterrence through a threat of retaliation' (DTR for short) is a reasonable strategy for governments to follow. In contrast to Gaycken (2011) again, we do not overestimate the suggestive power of the non-attribution-problem towards that issue. We argue that although non-attribution causes serious problems as described above, it has no impact on the strategic use of DTR. However, DTR causes problems on its own, because collectively 'played' as a strategy it runs into a complete prudential dilemma and therefore, it is self-defeating as a rational strategy.

The preliminary second section helps to specify our later arguments. We there start with a specification of non-attribution and its different dimension. Providing a useful distinction between different kinds of impossibilities of attribution, we can discriminate weak from strong assertions of non-attribution, which might be of interest for technical, legal and political professionals. Even in the weakest sense of impossibility of attribution all relevant problems can occur.
In the third section we provide a standard-taxonomy of the category of 'war' and reveal some important necessary conditions for the application of the term 'war'.
In the fourth section we set the floor for a logical clarification of a sound principle of self-defense. After showing that a sound principle of self-defense is impossible under conditions of non-attribution, we are able to formulate an interesting dilemma which is sufficient for arguing against the possibility of a rational legal regulation.
In the fifth section we firstly reject Gayckens' argument against DTR on logical grounds. We have to conclude that the strategy of DTR stays in the set of individually rational strategies. Secondly, this gives reason for concern that this strategy might constitute another dilemma.

2. A SPECIFICATION OF NON-ATTRIBUTION

To attribute a property to a system, we have to presuppose its possibility. It doesn't matter what kind of property you want to attribute, you carry the burden of proof of its possibility. The weight of the burden varies with the attribution you want to make. The same holds true for claiming the impossibility of non-attribution.
To sketch some conceptual difficulties of non-attribution, we now provide a useful distinction between ontological, epistemological, and empirical impossibilities of attribution in cyberwar and their normative ordering. This can help disambiguate popular arguments with different suggestive power regarding the alleged "theoretical impossibility" of non-attribution and its normative content. We argue that there are at least three types of impossibilities, which should be distinguished carefully.
First of all, there is the ontological level, where one could postulate an "ontological impossibility" of attribution, which would mean, that attribution is no meaningful category for describing anything. We suggest that attribution is ontologically possible. On the second level, we may ask if attribution is epistemologically

possible. Therefore we have to differentiate between the assumptions that attribution is possible or not for epistemological reasons, which constitute attribution-problems a priori (e.g. a violation against the principle of contradiction; "inscrutability of reference" (Quine (1960)); "strong diachronic emergence" (Stephan (2002)). We suggest that attribution-problems in cyberwar are not of that kind. They occur on much more practical, let's call it empirical level. On that third level, we can repeat the epistemic question, but refer to some empirical facts (e.g. conceptual consistency, classificatory practice, technical complexity, political implementation, legal rules, moral standards etc.) by answering the question of whether attribution is possible or not. We suggest that all arguments for the impossibility of attribution are special cases of this kind and all the relevant non-attribution-problems occur even on this level.

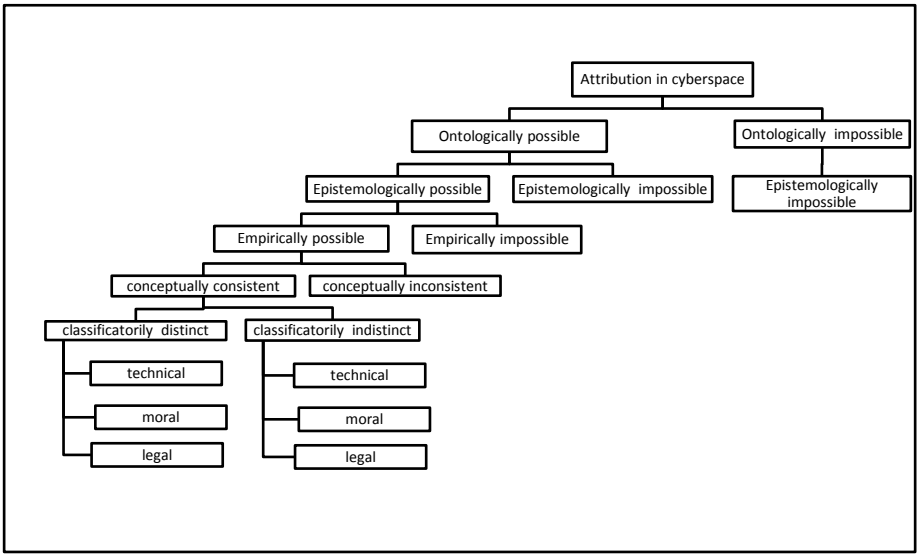

Figure 1: A Taxonomy of Attribution in Cyberspace

3. The Classical Definition of War and some logical clarifications

Let us now consider whether the strategy to reject the classification of 'cyberwar' towards current phenomena is successful by complaining that they don't fulfil the sufficient conditions one need to meet. To classify a special kind of war decisively, you than have to know which *differentiae specificae* are at hand to subsume the phenomenon rightly. As pointed out before, this rejecting is only successful under the possibility of attribution. In all standard cases it is presupposed that things at hand were undisputed. Some protagonist in the debate hold the opinion that there is

no and there will be no ‘cyberwar’ in the sense of international law for *classificatory reasons.* They argue that we *should not* talk about ‘cyberwar’, because the sufficient conditions to use that term were absent.

As stated above, the term ‘war’ gives rise to multidimensional definitional problems Therefore we should taxonomically discriminate purely *descriptively* with regard to the

a) Reasons/causes (e.g. religious, ideological, colonial, economic, freedom, independence, etc.)
b) Aims (e.g. intervention, sanctions, defense, attacking, liberation, etc.)
c) The types of conflicting parties (e.g. states, civil, etc.)
d) Used arms (e.g. conventional or non-conventional)
e) Domains (land, water, air, space, cyberspace)
f) Levels (strategic, operative, tactical)
g) Spatial and temporal
h) The starting point of conflicting parties (e.g. symmetric, asymmetric)
i) Structural reasoning (rational vs. irrational) and its
j) Legal status (permitted, forbidden, required)

And *normatively* concerning

k) Evaluative properties (good, bad, desirable) and
l) Deontic properties (morally legitimate, illegitimate, permitted, forbidden, required)

Obviously this kind of taxonomy is only applicable if attribution is a valid precondition. However, these problems refer only to the question of sufficient conditions of the term, not the necessary ones. On the latter we want to construe our argument. This different line of reasoning is concerned with the conceptual consistency of the term ‘cyberwar’ under conditions of non-attribution. All former approaches necessarily need to agree (at least implicitly) on the fulfilment of the following necessary conditions of the term ‘war’, which even can be found in all classical concepts of ‘war’ as “an actual, intentional and widespread armed conflict *between* political communities” (Orend (2008)) or complementary as an organized conflict, staged under use of weapons and violence/force of *at least two competing* parties, the aim of most wars is the betterment (recovery, attainment) of one’s own strategic situation respectively to prevent the opposite. The means used to that end implicitly or explicitly accept or directly intend a worsening of life conditions, physical violations or degradation of dignity, or the death of the *competing party* (see also Oppenheim (1952), Dinstein (2011)).

To accentuate them, we suggest the following logical requirements of the term ‘war’:

(1) It is conceptually impossible to be in a state of war without there being someone with whom one is at war. (Binary-Condition/Two-place-Condition)
(2) It is conceptually impossible to be in a state of war with oneself. (Non-Reflexivity-Condition)
(3) It is conceptually necessary that two conflicting parties are epistemically distinct in a stage of war. (Epistemic Distinction-Condition)

Without dispute ‘war’ denotes at least a binary relation „K_{xy}“ with $x \neq y$ and we hold conditions (1)-(3) evidently for true. But how can you say that a phenomenon you want to classify as an act of war even belongs to that category, when attribution of the attacker is claimed to be impossible? Are we really willing to sacrifice conditions (1)-(3) that easily?
We suggest that, without epistemic detectability, there is no way to use the term ‘war’ bijective without violating conditions (1)-(3). It further implies not only the suspension of the epistemic identification of the combatants, but rather constitutes a literally speaking ‘absolute war’ in the sense, that the disentanglement from the y-term of the two-place relation of ‘war’. This is because the two-place relation of war runs blank without any epistemic identification of the potential combatant.

4. The Impossibility of a Sound Principle of Self-Defense Under Non-Attribution

This section tries to highlight some difficulties regarding the possibility of a rational legal regulation of cyberwar. Assuming some plausible principles of self-defence, lying within the core of international law, we show that under the impossibility of attribution these principles become inconsistent and therefor cause a regulatory gap in international law, which ends up in our non-attribution-dilemma.
A sound concept of self-defence should require the following conditions:

(4) It is conceptually impossible to be in a state of self-defence without there being someone who attacks. (Binary-Condition/Two-place- Condition)
(5) It is conceptually impossible to be in a state of self-defence with oneself. (Non-Reflexivity-Condition)
(6) It is conceptually necessary that two conflicting parties are epistemically distinct in a stage of self-defence. (Epistemic Distinction-Condition)

To get a sound principle of self-defence, these conditions must be amended by the following widely accepted principles of international law:

(7) There is no unconditional right of self-defence (Self-Commitment to Certain (e.g. rational) Constraints)
(8) Any contractual party has the inherent (moral and legal) right to act in self-defense (e.g. to declare war), before/during/after an illegal attack from a stranger. (Weak Principle of Self-Defense)
(9) A victim has a legal duty to tolerate the offender’s enforcement power, so one cannot deduce a right of self-defense when one is offended by an act of self-defense. (No Self-Defense against Self-Defense)
(10) The self-defense has to be directed against the attacker and has to rely on the will to defend. (Strong Principle of Self-Defense)

(11) Mistakes of law must not justify self-defense. (Exclusion of Putative-Self-Defense as a reasonable justification)

The application of a sound principle of self-defense also presupposes a theory of causal connection between the behaviour of the potential offender and his victim by means of natural laws. If our theories of causality are limited to special phenomena (e.g. like what we dub as ontological or epistemological problems a priori) the application of our law is impossible. So we might add:

(12) Hypothetical causal connections cannot be incorporated in (international) criminal law. (Exclusion of Hypothetical Causes for Justification)[3]

(13) Mistakes of fact must not excuse self-defense. (Exclusion of Putative-Self-Defense as a reasonable excuse)

Because we don't want to bother you with a formal proof, we simply state here that the following argument has a similar structure like any impossibility-theorem. It relies on the insight that principles (4)-(7) and (10)-(13) cannot hold true at the same time under conditions of non-attribution. We assume that, once noticed, this inconsistency is easy to see. You either a) have to allow hypothetical or putative reasons for self-defence and cannot preclude the possibility that one act in self-defence for unsuitable reasons *or* b) you prohibit putative reasons and cannot act in self-defence. Tertium non datur. Beside the fact of its logical inconsistency, the regulatory gap leads to another high substantial dilemma, which we introduce now.
One main goal of international law is to prohibit the unjustified use of force, and accordingly to formulate some intersubjectively acceptable criteria for a breach of law. Conceptually inconsistent attribution (CIA for short) now points out that there cannot exist such a criterion. If CIA is valid, international law and its underlying principles are indistinguishable from pure arbitrariness. If the law allows any sanctions on these grounds, it lacks all of its legitimating power. To make things even worse, the principle of self-defense under non-attribution is indistinguishable from Putative-Self-Defense and therefore ruled out as a rational legal regulation.

> (NAD): The main goal of legal regulation is to avoid a stage of arbitrariness like anarchy with rational principles. If legal regulation permits war without epistemically justified reasons, it is indistinguishable from arbitrary anarchy. If Putative-Self-Defense is legal, any (false) allegation becomes a potential justifying reason to declare war. The point of CIA is that we cannot guarantee the exclusion of Putative-Self-Defense. When any conceptually inconsistent attributable cyberattack is a reason for self-defense, any regulation is pointless. Therefore CIA leads to a reductio ad absurdum for a rational concept of (epistemically justified) self-defense, because either it misses its own aim of rational regulation or it is indistinguishable from anarchy (or even worse leads to a "bellum omnium contra omnes").

[3] For example (Kühl (2008, 23))

5. DETERRENCE THROUGH A THREAT OF RETALIATION – A SELF-DEFEATING STRATEGY

Irrespectively to the above dilemma, rational strategies are relative to the actor's web of belief. Even in a world with non-attribution, one strong actor might not care about a sound principle of Self-Defence and might accept Putative-Self-Defense.
Retaliation as a strategy of deterrence, when chosen collectively, obviously leads to a stage of "bellum omnium contra omnes", which is presupposed to be collectively irrational. Rational regulation tried to avoid this inefficiency, but cannot guarantee it under the condition of CIA.
As mentioned in the introduction, a third challenge arises in the context of 'cyberwar' and non-attribution very often. It regards the question if deterrence through a threat of retaliation is a rational strategy under conditions of non-attribution. Gaycken (2010,1) postulates that "[…]deterrence is pointless without attribution. This is *logical* from a strategic point of view. If retaliation does not hit the attacker, he will not be deterred. […] Retaliation against the wrong actor is unjust and a crime of war. Thus attribution is a necessary condition of the law of war." (Gaycken 2010,1; our italics)
We argue that his conclusion is mistaken logically. Although we're convinced, that the possibility of attribution is a necessary condition for the application of the category of 'war' and a sound principle of self-defense, we show, that the impossibility of attribution does not lead to the alleged pointlessness of DTR. DTR is problematic for different reasons, for example it might lead back to a state of anarchy or in the worst case to a "bellum omnium contra omnes"[4].
Gaycken's argument in (2010,1) is simply not sound. His interpretation of the non-attribution-problem can be reconstructed as follows:

(i) "If retaliation does not hit the attacker, he will not be deterred" and
(ii) "Without proof, it is not possible for the victim state to retaliate […]", therefore
(iii) "Deterrence is pointless without attribution"

Aside from the fact that the argument is firstly not valid logically, (iii) simply doesn't follow from (i) and (ii), its premise (ii) is crucial here, because it does seemingly rule out the possibility that retaliation can hit the attacker. We claim, that the problem of non-attribution is described more adequately as the problem that the attacker cannot be identified in an epistemically reliable manner, so (ii) does not hold true and neglects the central problem. Gaycken does not only repeat this mistake, but he also extends this logical gap in (2011) by postulating that the probability of being identified is equal to zero, which doesn't follow from any

[4] It is worth noting that even Hobbes didn't use this term only for factual stages of armed conflict, but rather for stages of the mutual will to fight: "For WAR, consisteth not in battle only, or the act of fighting; but in tract of time, wherein the will to contend by battle is sufficiently known […]." (Leviathan 13, p. 113f.) (quoted in Kleemeier (2002, 129))

non-attribution-problem.[5] Under non-attribution we cannot ascribe any probability. However, non-attribution does not mean that there is "no risk" (Gaycken (2011,23)) of being punished. It only implies that there is no risk for the true attacker of being punished on an epistemically justified basis.

However, the question of faith here is, whether a non-attributable cyberattack leads to a reflective equilibrium, where the wish to deter through a threat of retaliation is deterred by international law. We will argue that it does not. States that do not accept principles (10)-(13) cannot be prosecuted by the law, when DTR can be justified by a permission-principle of the law or, alternatively, can be excused in the absence of responsibility.

In general there are two possibilities: DTR is either a) a special case of strong, active self-defense, which has to be subdivided into three other special cases, namely anticipatory[6], current and retaliatory cases or b) Putative-Self-Defense, which has to be discriminated with regard to "avoidable mistakes" and "unavoidable mistakes" of justification. If DTR hits the true attacker, it is a case of self-defense and eo ipso justified. The crucial case is, when DTR hits the wrong (e.g. innocent) state. Are there reasons to justify DTR in these circumstances? This question raises the second possibility that DTR is a case of Putative-Self-Defense (PSD for short). When DTR is a case of PSD, it is only justified if X made an "unavoidable mistake of fact or law".[7] It doesn't matter if we assume a direct intent or offense by negligence, because both were excluded in the case of unavoidable mistakes because of the impossibility of attribution. Guilt presupposes the absence of an unavoidable mistake of law and fact.

So under conditions of non-attribution it doesn't matter[8] if the possible defense runs through a justification according to certain principles[9] like § 15 ECHR, § 51 UN-Charta or as ultima ratio through an excuse by a 'mistake of fact' by[10], *because 'mistakes of fact' are systematically unavoidable under conditions of non-*

[5]There is another inconsistency when he criticizes the alleged identifications as nonserious with a probability of 80%, but he himself asserts it as "inevitable 50:50" (Gaycken (2011, 150)), which would mean, that it is still a decision under risk and not under uncertainty.

[6] An attack is current, if it immediatly starts, actual takes place or still continues. (Krey/Esser (2011, 196, our translation)). Some deny the right of anticipatory self-defense.

[7] Some doubt their existence in the core of criminal law (Kühl (2008), Heuchemer (2005))

[8] Does an unavoidable mistake of fact of an actor in cases of self-defense exclude the right of self-defense of the innocent offended? The German StGB suggests a duty to tolerate the offense when the offender reacts in a justified stage of emergency (even under a mistake of facts). In contrast, there is no duty, if the offense is merely excused by a stage of emergency. Therefore it does matter, which defense strategy is used.

[9] Or like in German Criminal Law through §§ 32, 34 StGB, §§ 228, 229, 230, 904 BGB

[10] In German Criminal Law a defense might run through §§ 16, 17 StGB or §§ 33, 35 StGB. As an excuse, the unavoidable mistake of fact or law does not lead to innocents, but to an exemption from punishment. As Kühl (2008, 414) points out, there exists a regulatory gap for cases like (unavoidable) mistakes of facts towards the permission of the action (= "Erlaubnistatumstandsirrtum"). However, there is an ongoing dispute how to apply a mistake of fact toward a permission of law (Krey/Esser (2011, 296), alternatively Heuchemer (2005))

attribution. To our knowledge this regulatory gap is mostly unknown in international law.[11]
On these grounds the "Exclusion of Putative-Self-Defense" is the crucial point of a slippery slope. So non-attribution does not only challenge the idea that the offender made a mistake in attribution, but that one cannot prove him to be mistaken. Therefore prosecution presupposes an epistemic point of view, from which the 'mistake' is testable. The potential impossibility of attribution simply denies such a point. If this crucial point of non-attribution holds true, this constitutes a fundamental "anything-goes"-justification-strategy for a casus belli, which consecutively constitutes the basis for the following fatal complete prudential dilemma.

If deterrence through a threat of retaliation stays in the set of individually rational strategies, the phenomenon of non-attribution might constitute a complete, iterated n-person prudential dilemma, which can be defined (according to Trapp (1998, 27; our translation)):

> Let S be a strategic interaction of players i from X = (1,…,n), who were able to choose an action of the set $H_i = \{h^i_1, \ldots, h^i_{m(i)}\}$ of alternatives. Therefore:
> D_1: according to X S is a complete prudential dilemma if and only if
> α) for any player there exists an action alternative, choosing which is rational, because $\forall h'^i(u_i(h_i)) > u_i(h'_i))$ holds true, so that their expected utility is higher than in any other alternative h'_i.
> β) at the same time there exists a vector $(h^1_+, h^2_+, \ldots, h^n_+)$ with $h^i \neq h^i_+$ (for i = 1, …, n) in S, for which holds that its collective realization through the players (1, …, n) would increase the payoff of every individual in comparison to the payoff of the vector $(h_1, h_2, \ldots, h_n)$, which due to α) will de facto eventuate.

It is characteristic for a complete prudential dilemma that its individually aggregated rational output is pareto-dominated by an outcome, which is not individually, but only collectively rational (e.g. a status of legal regulation). To make things even worse in such prudential dilemmas, no egoistic regulation mechanism exists (because it is complete!), to avoid its undesirable consequences.
Despite the existence of this dilemma, deterrence through a threat of retaliation stays in the set of individually rational strategies under specific conditions. Because there is no cogent argument that players might rationally believe that their own lives will not be „brutish and short" in anarchy. For this kind of player, DTR stays in the set of rational strategies, independently of whether attribution justifies anything or not. So it is important to discriminate between an individually rational regulation and a sound principle of self-defense and collectively rational strategies.

[11] Surely there are some disputes in academia regarding the theoretical assumptions underlying the principles of self-defense, but it underestimates the scope of non-attribution-problems. Moreover the dispute possibly constitutes a rational disagreement (e.g. the application of a strong or weak theory of guilt (Heuchemer (2005), Walter (2006), Ambos (2002, 2006)).

Therefore an adjustment of international law will not lead to a "softening" (Gaycken (2011, 198)), but rather to a reductio ad absurdum! Without attribution our term cyber'war' is pointless!

6. Conclusion

In this paper we argued, that the potential impossibility of attribution raises at least three challenges to international politics and international law. We referred to the closely related problems of the definition of 'cyberwar', rational legal regulation and deterrence through retaliation.

Although we're convinced that the possibility of attribution is a necessary condition for the application of the category of 'war' and a sound principle of self-defense in a rational law, it is no necessary condition for a strategy like DTR.

We showed that the problem to classify current phenomena under the category of 'cyberwar' is much more fundamental than thought so far. Only a change in the core concept of 'war' will enable us to talk about 'cyberwar' under conditions of non-attribution. This change is (hopefully) unlikely to happen.

The impossibility of sound principle of self-defense has a deep impact on the rational regulation and led us to an interesting non-attribution-dilemma, which is unsolved yet. It states that due to the impossibility of attribution an unsound principles of self-defense, at the utmost, lead back to a state of anarchy or "bellum omnium contra omnes" and eo ipso undermines the target of the legal regulation.

Regarding the connection of non-attribution and DTR we show its independence from each other. We argued that the inference from the non-attribution to the pointlessness of DTR was too hasty and not valid logically. Although we showed that the attribution problem has no impact on individually rational strategies of DTR, we could provide an interesting starting point of prudential-dilemma,which causes serious problems on its own.

7. References

Ambos, Kai. 2002. Der Allgemeine Teil des Völkerstrafrechts: Ansätze einer Dogmatisierung, Berlin: Duncker & Humblot

Ambos, Kai 2006. Internationales Strafrecht. Strafanwendungsrecht – Völkerstrafrecht – Europäisches Straftrecht, München: C.H. Beck

Dinstein, Yoram. 2011. War, Aggression and Self-defense. Cambridge

Gaycken, Sandro. 2010. "The Necessity of (Some) Certainty - A Critical Remark Concerning Matthew Sklerov's Concept of "Active Defense"." Journal of Military and Strategic Studies, vol. 12, issue 2, p.1-6

Gaycken, Sandro. 2011. Cyberwar – Das Internet als Kriegsschauplatz, Munich: Open Source Press

[,left blank intentionally'] 2012.

Hayden, Michael V.. 2011. The Future of Things Cyber
Heuchemer, Michael. 2005. Der Erlaubnistatbestandsirrtum, Berlin: Duncker & Humblot
Hoyer, Werner. 2011. Accessed January 10 2012 http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2011/111213-StM_H_Cybersecurity.html
Kleemeier, Ulrike. 2002. Grundfragen einer philosophischen Theorie des Krieges, Berlin,
Kosina, Karin. 2012. Wargames in the Fifth Domain. Vienna http://kyrah.net/da/wargames.pdf
Krey, Volker/ Esser, Robert. 2011. Deutsches Strafrecht – Allgemeiner Teil. Esser, Robert (ed.), Stuttgart: Kohlhammer
Lindner, Felix. 2012. We Came In Peace – They Don't. Hackers vs. Cyberwar. Wien (Lecture held at the DeepSec Conference 2012)
Kühl, Christian. 2008. Strafrecht – Allgemeiner Teil. München: Vahlen
Münkler, Herfried. 2004. Die Neuen Kriege, Reinbeck bei Hamburg: Rowohlt
Oppenheimer, Lassa F.L. 1952. International Law. London
Orend, Brian. 2008. 'War'. The Stanford Enyclopedia of Philosophy, Edward N. Zelta (ed.), URL = http://plato.stanford.edu/archives/fall2008/entries/war/
Quine, Willard v. O.. 1960. Word and Object, Massachusetts: MIT Press
Stephan, Achim. 2002. "Emergentism, Irreducibility, And Downward Causation." Grazer Philosophische Schriften 65: 77-93
Trapp, Rainer. 1998. Klugheitsdilemmata und die Umweltproblematik, Munich: Schöningh
Walter, Tonio. 2006. Der Kern des Strafrechts. Die allgemeine Lehre vom Verbrechen und die Lehre vom Irrtum, Tübingen: Mohr Siebeck
Ziolkowski, Katharina. 2012. Cybersicherheit, Cyberkonflikt und die Aufgaben der NATO CCDCOE, Osnabrück (Lecture held at European Legal Studies Instiute)