Stefanie Schmahl, Cybersecurity, in: Freiheit und Regulierung in der Cyberwelt – Rechtsidentifikation zwischen Quelle und Gericht, Berichte DGIR Bd. 47, Heidelberg 2016.

Summary

by Prof. Dr. Stefanie Schmahl, Würzburg

I. Empirical Diagnosis: Level of Potential Threat in Cyberspace

1. The number of malicious computer network operations has significantly increased during recent years. Estonia, Georgia, Iran, the Ukraine and the United States of America have been amongst the victims of the most spectacular cyber attacks. Until today, it remains however unclear who was the author or the entity responsible for those harmful cyber operations.

II. Terminological Delimitations: Cybersecurity as a Means to Combat Detrimental Computer Network Operations

2. Although disastrous harm has not yet been produced, there is no doubt that computer network operations have a high potential of threatening the international stability. The international legal order is therefore called upon to find an answer to these threats. A pivotal concern in this regard is the question which defensive and preventive mechanisms against hostile cyber attacks originating from a foreign country are permitted. As a notion, cybersecurity must not be equated with "cyber war", since it encompasses further areas such as cyber terrorism.

3. The techniques used for detrimental computer network operations are manifold; in essence one can distinguish between non-intrusive and intrusive methods of operation. Non-intrusive cyber methods do not infiltrate the computer system but diminish or hamper its functionality. Intrusive cyber operations, by contrast, directly penetrate the attacked systems of information technology. The consequences remain intrinsic in cases where computer data are merely spied out (so-called "computer network exploitation"). If, however, data are converted or deleted, these operations regularly produce external effects and, in extreme cases, they might even have destructive consequences like the loss of life, of physical integrity or of property (so-called "computer network attack").

4. Despite their different types and characteristics, all cyber operations disclose some structural commonalities which challenge the existing basic principles of international law. The enormous speediness, the neutrality and the transnational ubiquity of data transfer, the amorphous effects which can be produced by computer network operations and the dual use-character of the information technology infrastructure count among these commonalities. The lacking technological controllability of some malware, the State-like abilities of certain non-State actors and, in particular, the possibility of conducting cyber attacks from great distances and in an anonymous or technically masked way raise further problems.

III. Legal Findings: Rules Applicable in the Field of Cybersecurity

5. As has been the case with all technical achievements in the past, it is hard to find positive regulations and normative assessments also in the complex realm of cybersecurity. The canon of international treaties at disposal does not offer a tailor-made solution for the challenges produced by this novel phenomenon. Likewise, State practice does not

offer, at least for the time being, a sufficiently consistent pattern to be analysed in terms of a *jus digitale emergens*. Therefore, it has to be considered whether the digital risks may be brought under control by a flexible and dynamic interpretation of the basic rules of international law. In the alternative, one has to consider the option that even a modern evaluation of these rules might remain too vague and indeterminate with the result that there could be a need for elaborating specific provisions on cybersecurity.

IV. Possibilites of Therapy *de lege lata et ferenda*: Security Mechanisms in Cyberspace

1. Defensive Measures

a) Self-Defence and Countermeasures

6. Certain manifestations of cyber operations comply with the notion of armed force. To that end, it is sufficient that damage be inflicted in an indirect way; it has not to be destructive in a strictly literal sense. However, in order to be equated with the use of force, cyber operations must have an impact similar to conventional kinetic weapons. Therefore, an irresistible external physical damage to objects or persons is necessary.

7. Not every use of armed force gives the right to self-defence. In order to amount to an armed attack, the "scale and effects" of an operation are to be considered and must be significant. When adapting these shorthand terms to cyber operations it appears that the malware utilised must produce physically destructive effects on the adversary of a remarkable level.

8. Operations which do not trespass the threshold of an armed attack but qualify as coercion may constitute unlawful interventions into domestic affairs or violations of the prohibition on the use of force. In those cases, State may resort merely to (non-military) countermeasures. This is, in principle, also valid in the event of accumulated cyber incidents each of which falls short of an armed attack (so-called "cyber campaigns"). Since cyber operations are usually veiled and their effects are frequently not immediately apparent, it is difficult, if not impossible to substantially demonstrate a serial context within the meaning of the "pin prick" theory or the doctrine of accumulation of events.

9. In a similar vein, it is virtually impossible, in the case of malicious cyber attacks, that the criteria of preventive self-defence be fulfilled. Against the background of the *Webster* formula, it is not sufficient that destructive malware has merely been deposited on a computer or filed on a data processor. An "imminent cyber attack" may be assumed at the earliest when there is a verifiable infiltration in the dataset of the victim State. In addition, inactive "sleeping" malware, once detected, might well be isolated or otherwise rendered harmless so as to avert the danger and exclude recourse to military means.

b) Questions of Attribution

10. The question of who is the right addressee of a countermeasure raises particular problems when cyber operations are conducted by non-State actors without formal State authorization or State approval. A wrongful act may well be attributed to a State on the basis of a merely factual relationship, supposed that a non-State actor is guided or controlled by the State authorities and acts as their "extended arm". However, individual hackers who act on their own initiative and use hacking tools that can be freely

found on the internet do not fulfil these conditions. Even the ICTY does not extend the "overall control" standard, which is significantly broader that the "effective control" test applied by the ICJ, to single individuals or unorganised groups for attributing their conduct to a State. Only in cases where a State positively acknowledges, honours or supports the action undertaken by private hackers, one might conclude differently. Under those circumstances, a substantial involvement of the State cannot be excluded from the outset, and, depending on the surrounding conditions, even a retroactive attribution to the "background State" may be considered.

11. Strictly separate therefrom are those constellations where a State does simply not prevent cyber attacks which emanate from private hacktivists autonomously acting on its territory. In this context, the State does not comply with its duty to protect, and the failure to exercise due diligence in order to prevent such operations from occurring qualify as a sufficient basis for attribution. According to the standard of due diligence, States are obliged to provide for adequate preventive and repressive measures in order to inhibit and to punish, as far as possible, detrimental cyber operations taking place under their territorial and personal jurisdiction. Infringements of this duty may constitute a wrong of its own against which the injured State may resort to countermeasures. A right to military defence, however, has to be rejected. The same is true for accountability conditions stricter than due diligence. In particular, an obligation of result or the standard of constructive knowledge ("should have known") would utterly overburden any State since it is not able to know or to investigate on every harmful data movement on its territory.

12. If neither participation nor acquiescence of the State where a cyber operation originates from is verifiable, it is only in exceptional situations of necessity that the victim State is allowed, without or against the will of the territorial State, to expand its countermeasures on the territory where the hacktivists are presumed to reside. A different conclusion has to be drawn, however, with regard to fighting cyber terrorists and their facilities with targeted military means. In its Wall Advisory Opinion, the ICJ has once again stressed the necessity of attributing a wrongful act to a State in order to justify a situation of self-defence.

c) Standards of Evidence

13. Anonymous or masked cyber attacks pose an outstanding challenge for the lawfulness of countermeasures. Every form of defensive measures presupposes that both attack and attacker are unambiguously identifiable. According to the principles of State responsibility, the burden of proof rests with the victim State.

14. From a legal perspective, trusting that future technological developments will facilitate the identification of the attacker is no satisfactory option. Just as little convincing is the view according to which cyber operations allow for a deviation from the prerequisite of "reasonable certainty" by replacing it with the condition of a mere rebuttable presumption. Such a dispensation from causality strands and rules of evidence finds no support either in international customary or in international treaty law. The "duty to protect-doctrine" must not be intermingled with the law of countermeasures. The erroneous excercise of the right to self-defence, namely when the defence is directed against an incorrect addressee, bears a high potential of escalation. Even the arbitrary recourse to non-military countermeasures involves dangers for the international security.

2. Offensive and Preventive Security Measures

15. Instead of applying defensive measures which necessarily lose effects when cyber operations are conducted in a veiled way, it seems to be favourable to consult the precautionary principle which is common to the area of international environmental law and to the field of international regulations of technical issues. The precautionary principle reacts to states of general dangers as well as to situations of nescience and aims at minimizing risks at a previous stage. Such measures of precaution are familiar to the corpus of international humanitarian law, too.

16. A comprehensive prohibition of developing and applying cyber operations is out of question. The range of possible modes, shapes and characteristics of cyber methods is far too broad, and the effective control of such a far-reaching proscription is simply not possible. The draft of a "Convention on International Information Security" which has been recently submitted by Russia, China and other States, refrains from a complete prohibition. Still, it runs the risk of curtailing the individual freedom of speech and of information.

17. The idea of precaution is not limited to a complete prohibition of conduct fraught with risk. The precautionary principle also includes low-threshold measures. Furthermore, it involves the initiator of the perilous situation. The precautionary principle might even lead to due diligence obligations addressed at all States. Such a collective "duty to prevent cyber attacks" is conceptually possible by establishing, e.g., legally binding maxims of conduct such as mutual duties to information, consultation, risk estimate and the duty to legal and administrative cooperation. To the extent that such standards of conduct are consented to on the international level, *erga omnes* obligations can emerge, which, in case of a violation, might even entail the duty to tolerate defensive mechanisms taken by other States.

V. Synthesis and Conclusion: The International Law of Cybersecurity as a Cross-Sectional Subject Matter

18. The international law of cybersecurity is a cross-sectional field that puts to test the panoply of rules and principles of international law. Due to its technological challenges, it also depends on gains in interdisciplinary knowledge. From the international law perspective, however, it has to be underlined that a fundamental paradigm shift in terms of formulating new substantial legal parameters for cybersecurity is inappropriate. It is hard to find a consensus on the criteria for a noxious cyber operation to be established; it is not by coincidence that the Council of Europe Cybercrime Convention leaves the contracting States a wide margin of appreciation.

19. The novel threats resulting from information technology are to be coped with on the basis of the existing legal instruments which are well legitimized because they serve and aim at avoiding armed conflicts. Concepts and notions such as "intervention", "force" or "armed attack" can be dynamically interpreted in order to match with the realities of modern information societies.

20. Even the possibilities to veil an operation or to stay anonymous which are typical for the sphere of the internet do not render the main principles of international law obsolete. *De facto* shortcomings, in particular with regard to identification and attribution, are common to other legal fields such as combating terrorism and asymmetric warfare. The States, whose importance as guarantors for the security in cyberspace is constantly

increasing, should and shall intensify their intergovernmental efforts of cooperation in order to close the obvious protection gaps. Unlike the establishment of new substantial legal regimes, *erga omnes* maxims of conduct with the objective of minimizing the risk of detrimental computer network operations are comparatively fast negotiable. At the same time, they may also be expected to withstand the racy technological development.