The
Federal Government

On the Application of International Law in Cyberspace

Position Paper* – March 2021, to be annexed to the Report of the 2021 United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security

I. Introduction

Cyber activities have become an **integral part of international relations.** The vast interconnectedness of networks, technologies and cyber processes across borders has brought societies and individuals from different nations closer together and has opened up new opportunities for cooperation among both State and non-State actors. At the same time, States and societies have grown highly dependent on the functioning of IT infrastructures. This has created new vulnerabilities. In cyberspace, only limited resources are often needed to cause significant harm. This poses security threats for States and societies. Harmful cross-border cyber operations, both by State and non-State actors, can jeopardize international stability.

Germany is firmly convinced that **international law is of critical importance when dealing with opportunities and risks related to the use of information and communication technologies in the international context.** As a main pillar of a rules-based international order, international law as it stands provides binding guidance on States' use and regulation of information and communication technologies and their defence against malicious cyber operations. In particular, the UN Charter fulfils a core function with regard to the maintenance of international peace and security – also in relation to cyber activities. In this regard, Germany reemphasizes its conviction that **international law, including the UN Charter and international humanitarian law (IHL), applies without reservation in the context of cyberspace.**[1]

This paper discusses selected aspects of the interpretation of certain core principles and rules of international law in the cyber context.[2] Germany thereby aims to **contribute to the**

---

* The position paper has been prepared by the German Federal Foreign Office and the German Federal Ministry of Defence in cooperation with the German Federal Ministry of the Interior, Building and Community.

1 See also United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report of 24 June 2013, UN Doc. A/68/98, para. 19 and cf. report of 22 July 2015, UN Doc. A/70/174, paras. 24, 25; General Assembly resolution 70/237, Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/70/237, 30 December 2015.

2 The choice of rules and principles discussed is necessarily selective and no conclusions regarding Germany's legal position can be drawn from any actual or perceived omission to mention certain rules, principles, criteria or legal considerations.

ongoing discussion on the modalities of application of international law – most of which predates the development and rise of information and communication technologies – in the cyber context. The paper also intends to foster **transparency, comprehensibility and legal certainty** with regard to an important aspect of foreign affairs. The explanations take into account, *inter alia,* the 2013 and 2015 reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.[3] They are based on applicable international law and in this regard consider, to a significant degree, the findings of independent international law experts recorded in the Tallinn Manual 2.0.[4]

For the purpose of this paper, 'cyber processes' are events and sequences of events of data creation, storage, processing, alteration or relocation through means of information technology. The term 'cyber infrastructure' refers to all types of hardware and software components, systems and networks which allow for the implementation of 'cyber processes'. This includes '[t]he communications, storage, and computing devices upon which information systems are built and operate.'[5] 'Cyber activities' are 'cyber processes' instigated by users of cyber infrastructure. The term 'cyber operation' more narrowly refers to the 'employment of cyber capabilities to achieve objectives in or through cyberspace.'[6] 'Cyberspace' itself is understood here as the conglomerate of (at least partly interconnected) 'cyber infrastructures' and 'cyber processes' in the above-mentioned sense. In this paper, the adjective 'malicious', when used to describe certain activities in cyberspace, is not purported to carry a technical legal meaning.

II. Obligations of States derived from the United Nations Charter

a) Sovereignty

The legal principle of **State sovereignty[7] applies to States' activities with regard to cyberspace.[8]** State sovereignty implies, *inter alia,* that a State retains a right of regulation, enforcement and adjudication (jurisdiction) with regard to both persons engaging in cyber activities and cyber infrastructure on its territory.[9] It is limited only by relevant rules of international law, including international humanitarian law and international human rights

3 See above, note 1.

4 Schmitt, M. (gen. ed.)/Vihul, L. (man. ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, 2nd edition, Cambridge University Press 2017. The Tallinn Manual 2.0 is a paper created by independent experts and constitutes neither a document stating NATO positions nor a position paper by States. In the following, references to the Tallinn Manual 2.0 are made for information purposes only and do not necessarily constitute an endorsement of the referenced text by the German government.

5 Tallinn Manual 2.0 (note 4), Glossary (p. 564).

6 Ibid.

7 The legal principle of State sovereignty is enshrined – in conjunction with the notion of equality of States – in Art. 2 para. 1 of the UN Charter.

8 See also UN Group of Governmental Experts, reports of 2013 and 2015 (note 1), paras. 20 and 27, 28 (b) respectively; Tallinn Manual 2.0 (note 4), rule 1.

9 A State's jurisdiction may under certain conditions apply to situations beyond its borders, i.e. according to the principles of active and of passive nationality as well as universality.

law. Germany recognizes that due to the high degree of cross-border interconnectedness of cyber infrastructures, a State's exercise of its jurisdiction may have unavoidable and immediate repercussions for the cyber infrastructure of other States.[10] While this does not limit a State's right to exercise its jurisdiction, **due regard has to be given to potential adverse effects on third States.**

By virtue of sovereignty, a State's **political independence** is protected and it retains the right to freely choose its political, social, economic and cultural system. *Inter alia,* a State may generally decide freely which role information and communication technologies should play in its governmental, administrative and adjudicative proceedings. Foreign interference in the conduct of elections of a State may under certain circumstances constitute a breach of sovereignty or, if pursued by means of coercion, of the prohibition of wrongful intervention.[11] Moreover, by virtue of its sovereignty, a State may decide freely over its foreign policy also in the field of information and communication technologies.[12]

Furthermore, a State's **territorial sovereignty** is protected. Due to the rootedness of all cyber activities in the actions of human beings using physical infrastructure, cyberspace is not a deterritorialized forum.[13] In this regard, Germany underlines that there are no independent 'cyber borders' incongruent with a State's physical borders which would limit or disregard the territorial scope of its sovereignty. Within its borders, a State has the exclusive right – within the framework of international law – to fully exercise its authority, which includes the protection of cyber activities, persons engaging therein as well as cyber infrastructures in the territory of a State against cyber and non-cyber-related interferences attributable to foreign States.[14]

As a corollary to the rights conferred on States by the rule of territorial sovereignty, States are under an 'obligation not to allow knowingly their territory to be used for acts contrary to the rights of other States'[15] – this generally applies to such use by State and non-State actors. The **'due diligence principle',** which is widely recognized in international law, is applicable to the cyber context as well and gains particular relevance here because of the vast interconnectedness of cyber systems and infrastructures.

Germany agrees with the view that **cyber operations attributable to States which violate the sovereignty of another State are contrary to international law.**[16] In this regard, State sovereignty constitutes a legal norm in its own right and may apply directly as a general norm also in cases in which more specific rules applicable to State behaviour, such as the

---

10 For example, restrictive regulatory or enforcement activities regarding important internet nodes in the territory of one State may seriously impair the functioning of networks of other States.

11 See below, at II.b).

12 See Tallinn Manual 2.0 (note 4), rule 3 ('external sovereignty').

13 Ibid., rule 1, commentary, para. 5.

14 Ibid., rule 2 with commentary, para. 2.

15 See International Court of Justice (ICJ), Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgement of 9 April 1949, I.C.J. Reports 1949, 4, 22; Permanent Court of Arbitration (PCA - administering institution), Island of Palmas Case (or Miangas), United States of America v. The Netherlands, Arbitral Award (M. Huber) of 4 April 1928, (1928) II RIAA 829, 839.

16 Cf. Tallinn Manual 2.0 (note 4), rule 4.

prohibition of intervention or the use of force, are not applicable. Violations of State sovereignty may *inter alia* involve its territorial dimension; in this regard, the following categories of cases may be relevant (without excluding the possibility of other cases):

Germany essentially concurs with the view proffered, *inter alia,* in the Tallinn Manual 2.0 that cyber operations attributable to a State which lead to **physical effects and harm in the territory of another State** constitute a violation of that State's territorial sovereignty.[17] This encompasses physical damage to cyber infrastructure components *per se* and physical effects of such damage on persons or on other infrastructure, i.e. cyber or analogue infrastructure components connected to the damaged cyber component or infrastructure located in the vicinity of the damaged cyber infrastructure (provided a sufficient causal link can be established).

Germany generally also concurs with the view expressed and discussed in the Tallinn Manual 2.0 that certain effects in form of **functional impairments** with regard to cyber infrastructures located in a State's territory may constitute a violation of a State's territorial sovereignty.[18] In Germany's view, this may also apply to certain substantial non-physical (i.e. software-related) functional impairments. In such situations, an evaluation of all relevant circumstances of the individual case will be necessary. If functional impairments result in substantive secondary or indirect physical effects in the territory of the target State (and a sufficient causal link to the cyber operation can be established), a violation of territorial sovereignty will appear highly probable.[19]

In any case, **negligible** physical effects and functional impairments below a certain impact threshold cannot – taken by themselves – be deemed to constitute a violation of territorial sovereignty.

Generally, the fact that a piece of **critical infrastructure** (i.e. infrastructure which plays an indispensable role in ensuring the functioning of the State and its society) or a company of special public interest in the territory of a State has been affected may indicate that a State's territorial sovereignty has been violated. However, this cannot in and of itself constitute a violation, *inter alia* because uniform international definitions of the terms do not yet exist. Also, cyber operations in which infrastructures and/or companies which do not qualify as 'critical' or 'of particular public interest' are affected may likewise violate the territorial sovereignty of a State.

b) Prohibition of wrongful intervention

The prohibition of a wrongful intervention between States[20] is not explicitly mentioned in the UN Charter. However, it is a corollary of the sovereignty principle, can be derived from art. 2

17 Tallinn Manual 2.0 (note 4), rule 4, commentary, para. 11.
18 Cf. ibid., rule 4, commentary, para. 13 ("loss of functionality").
19 Cf. ibid.
20 On its applicability in the cyber context see also UN Group of Governmental Experts, report of 2015 (note 1), para. 28 (b).

para. 1 UN Charter and is grounded in customary international law. Generally, for State-attributable conduct to qualify as a wrongful intervention, the conduct must **(1) interfere with the *domaine réservé* of a foreign State and (2) involve coercion.**[21] Especially the definition of the latter element requires further clarification in the cyber context.

In its Nicaragua judgement, the International Court of Justice (ICJ) held that *'[t]he element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.'*[22] Malicious cyber activities will only in some cases amount to direct or indirect use of force.[23] However, measures below this threshold may also qualify as coercive. Generally, Germany is of the opinion that cyber measures may constitute a prohibited intervention under international law if they are **comparable in scale and effect to coercion in non-cyber contexts.**

Coercion implies that a State's internal processes regarding aspects pertaining to its *domaine réservé* are significantly influenced or thwarted and that its will is manifestly bent by the foreign State's conduct. However, as is widely accepted, **the element of coercion must not be assumed prematurely.** Even harsher forms of communication such as pointed commentary and sharp criticism as well as (persistent) attempts to obtain, through discussion, a certain reaction or the performance of a certain measure from another State do not as such qualify as coercion. Moreover, the acting State must intend to intervene in the internal affairs of the target State[24] – otherwise the scope of the non-intervention principle would be unduly broad.

In the context of wrongful intervention, the problem of **foreign electoral interference by means of malicious cyber activities** has become particularly virulent. Germany generally agrees with the opinion that malicious cyber activities targeting foreign elections may – either individually or as part of a wider campaign involving cyber and non-cyber-related tactics – constitute a wrongful intervention.[25] For example, it is conceivable that a State, by **spreading disinformation via the internet, may deliberately incite violent political upheaval, riots and/or civil strife** in a foreign country, thereby significantly impeding the orderly conduct of an election and the casting of ballots. Such activities may be comparable in scale and effect to the support of insurgents and may hence be akin to coercion in the above-mentioned sense. A detailed assessment of the individual case would be necessary.

Also, the **disabling of election infrastructure and technology** such as electronic ballots, etc. by malicious cyber activities may constitute a prohibited intervention, in particular if this

---

21 International Court of Justice (ICJ), Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America), Merits, Judgement of 27 June 1986, I.C.J. Reports 1986, 14, para. 205.

22 Ibid.

23 See below, at II.c).

24 Cf. Tallinn Manual 2.0 (note 4), rule 66, commentary, para. 27.

25 See also above, II.a).

compromises or even prevents the holding of an election, or if the results of an election are thereby substantially modified.

Furthermore, beyond the mentioned examples, cyber activities targeting elections may be comparable in scale and effect to coercion if they **aim at and result in a substantive disturbance or even permanent change of the political system of the targeted State,** i.e. by significantly eroding public trust in a State's political organs and processes, by seriously impeding important State organs in the fulfilment of their functions or by dissuading significant groups of citizens from voting, thereby undermining the meaningfulness of an election. Due to the complexity and singularity of such scenarios, it is difficult to formulate abstract criteria. Discussions in this context are still ongoing.

c) Prohibition of the use of force

So far, the vast majority of malicious cyber operations fall outside the scope of 'force'. However, **cyber operations might *in extremis* fall within the scope of the prohibition of the use of force** and thus constitute a breach of art. 2 para. 4 UN Charter.

The ICJ has stated in its Nuclear Weapons opinion that Charter provisions *'apply to any use of force, regardless of the weapons employed.'*[26] Germany shares the view that with regard to the definition of 'use of force', emphasis needs to be put on the **effects rather than on the means** used.

Cyber operations can cross the threshold into use of force and cause significant damage in two ways. Firstly, they can be **part of a wider kinetic attack.** In such cases they are one component of a wider operation clearly involving the use of physical force, and can be assessed within the examination of the wider incident. Secondly, outside the wider context of a kinetic military operation, cyber operations can **by themselves cause serious harm and may result in massive casualties.**

With regard to the latter case, Germany shares the view expressed in the Tallinn Manual 2.0: the threshold of use of force in cyber operations is defined, in analogy to the ICJ's Nicaragua judgement,[27] by the **scale and effects** of such a cyber operation.[28] Whenever scale and effects of a cyber operation are comparable to those of a traditional kinetic use of force, it would constitute a breach of art. 2 para. 4 UN Charter.

The determination of a cyber operation as having crossed the threshold of a prohibited use of force is a **decision to be taken on a case-by-case basis.** Based on the assessment of the scale and effects of the operation, the broader context of the situation and the significance of the malicious cyber operation will have to be taken into account. Qualitative criteria which may play a role in the assessment are, *inter alia,* the severity of the interference, the

---

[26] International Court of Justice (ICJ), Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, I.C.J. Reports 1996, 226, para. 39.

[27] ICJ, Military and Paramilitary Activities in and against Nicaragua (note 21), para. 195.

[28] Tallinn Manual 2.0 (note 4), rules 69, 71.

immediacy of its effects, the degree of intrusion into a foreign cyber infrastructure and the degree of organization and coordination of the malicious cyber operation.

III. Obligations of States under international humanitarian law (IHL)

a) Applicability of IHL in the cyber context

Germany reiterates its view that **IHL applies to cyber activities in the context of armed conflict.**[29] The fact that cyberspace as a domain of warfare was unknown at the time when the core treaties of IHL were drafted does not exempt the conduct of hostilities in cyberspace from the application of IHL. As for any other military operation, IHL applies to cyber operations conducted in the context of an armed conflict independently of its qualification as lawful or unlawful from the perspective of the *ius ad bellum.*

An **international armed conflict** – a main prerequisite for the applicability of IHL in a concrete case – is characterized by armed hostilities between States. This may also encompass hostilities that are partially or totally conducted by using cyber means. Germany holds the view that cyber operations of a non-international character, e.g. of armed groups against a State, which reach a sufficient extent, duration, or intensity (as opposed to acts of limited impact) may be considered a **non-international armed conflict** and thereby also trigger the application of IHL.[30]

At the same time, cyber actions can become **part of an ongoing armed conflict.** In order to fall within the ambit of IHL, the cyber operation must show a **sufficient nexus with the armed conflict,**[31] i.e. the cyber operation must be conducted by a party to the conflict against its opponent and must contribute to its military effort.[32]

Cyber operations between a non-State actor and a State alone *may* provoke a non-international armed conflict. However, this will only seldom be the case due to the level of intensity, impact and extent of hostilities required. Thus, activities such as a large-scale intrusion into foreign cyber systems, significant data theft, the blocking of internet services and the defacing of governmental channels or websites will usually not singularly and in themselves bring about a non-international armed conflict.[33]

---

29 Cf. also ibid., rule 80.

30 Generally, a non-international armed conflict is characterized by 'protracted armed violence between governmental authorities and organized armed groups or between such groups within a State', International Criminal Tribunal for the former Yugoslavia (ICTY), Prosecutor v. Dusko Tadić (aka 'Dule'), Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Appeals Chamber), Case No. IT-94-1, 2 October 1995, para. 70. On the definitions of international and non-international armed conflict in the cyber context, cf. also Tallinn Manual 2.0 (note 4), rules 82 and 83.

31 Tallinn Manual 2.0 (note 4), rule 80, commentary, para. 5.

32 See on the discussion ibid., rule 80, commentary, paras. 5, 6.

33 Ibid., rule 83, commentary, paras. 2, 7 and 8.

b) The fundamental principles of IHL limiting the recourse to cyber operations in the context of an armed conflict

The basic principles governing the conduct of hostilities, including by cyber means, such as the principles of distinction, proportionality, precautions in attack and the prohibition of unnecessary suffering and superfluous injury, apply to cyber attacks in international as well as in non-international armed conflicts.

Germany defines a **cyber attack in the context of IHL as an act or action initiated in or through cyberspace to cause harmful effects on communication, information or other electronic systems, on the information that is stored, processed or transmitted on these systems or on physical objects or persons.**[34] The occurrence of physical damage, injury or death to persons or damage or destruction to objects comparable to effects of conventional weapons is not required for an attack in the sense of art. 49 para. 1 Additional Protocol I to the Geneva Conventions.[35] However, the mere intrusion into foreign networks and the copying of data does not constitute an attack under IHL.

(1) The prohibition of indiscriminate attacks and cyber operations

The principle of distinction obliges States to differentiate between military and civilian objects, as well as between civilians, on the one hand, and combatants, members of organized armed groups and civilians taking direct part in hostilities, on the other hand. While IHL does not prohibit an attack on the latter, civilians (not taking direct part in hostilities) and civilian objects must be spared.

Civilians operating in cyberspace can be considered as taking direct part in hostilities with the result of losing their protection from attack and the effects of the hostilities, provided the following conditions are met: Their acts are likely to adversely affect the military operations or military capacity of a party, there is a direct causal link between their acts and the adverse effects and the acts are specifically designed to inflict harm in support of a party to an armed conflict and to the detriment of another (belligerent nexus).[36] Thus, Germany agrees with the view that, for example, 'electronic interference with military computer networks [...], whether through computer network attacks or computer network exploitation, as well as wiretapping [...] [of an] adversary's high command or transmitting tactical targeting information for an attack', could suffice in order to consider a civilian person as directly participating in hostilities.[37]

Following the same logic, a **civilian object like a computer, computer networks, and cyber infrastructure, or even data stocks,** can become a military target, if used either for

---

34 See also NATO Terminology Tracking Form (TTF) 2015-0028 (last entry 2019-02-12).

35 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3.

36 International Committee of the Red Cross (ICRC)/Melzer, N., Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law, 2009, available at www.icrc.org, p. 16.

37 Ibid., p. 48 (footnotes omitted).

both civilian and military purposes or exclusively for the latter. However, in cases of doubt, the determination that a civilian computer is in fact used to make an effective contribution to military action may only be made after a careful assessment.[38] Should substantive doubts remain as to the military use of the object under consideration, it shall be presumed not to be so used.[39]

The benchmark for the application of the principle of distinction is the **effect caused by a cyber attack,** irrespective of whether it is exercised in an offensive or a defensive context. Thus, **computer viruses designed to spread their harmful effects uncontrollably** cannot distinguish properly between military and civilian computer systems as is required under IHL and their use is therefore prohibited as an indiscriminate attack. In contrast, **malware that spreads widely into civilian systems but damages only a specific military** target does not violate the principle of distinction. Given the complexity of cyber attacks, the limited options to comprehensively appraise their nature and effects and the high probability of an impact on civilian systems, having recourse to the appropriate expertise to assess potential indiscriminate effects throughout the mission planning process is of key importance to Germany.

A cyber attack directed against a military target which is nevertheless expected to cause **incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof,** is also prohibited under IHL if such incidental effects would be excessive in relation to the concrete and direct military advantage anticipated.[40] If a cyber attack is executed in conjunction with other forms of military action, such as attacks with conventional weapons directed against the same installation, the military advantage and the collateral damage must be considered with regard to the 'attack [...] as a whole and not only [...] [with regard to] isolated or particular parts of the attack.'[41]

Assessing collateral damage and incidental injury or loss of life when conducting a proportionality analysis can be even more difficult in the context of cyber operations as compared to more traditional, i.e. physical, means or methods of warfare. This however does not discharge those planning and coordinating attacks from taking into account their foreseeable direct and indirect effects.

38 Tallinn Manual 2.0 (note 4), rule 102.

39 Additional Protocol I (note 35), art. 52 para. 3.

40 Additional Protocol I (note 35), art. 51 para. 5 (b); Tallinn Manual 2.0 (note 4), rule 113.

41 Declarations made by Germany at the time of ratification of Additional Protocol I (note 35), see 'Bekanntmachung über das Inkrafttreten der Zusatzprotokolle I und II zu den Genfer Rotkreuz-Abkommen von 1949' (Notice concerning the entry into force of Additional Protocols I and II to the 1949 Geneva Red Cross Conventions), 30 July 1991, BGBl. 1991 II, 968, 969; Tallinn Manual 2.0 (note 4), rule 113, commentary, para. 10.

(2) The obligation to take precaution in planning and executing a cyber attack

A corollary to the prohibition of indiscriminate cyber attacks is the duty to take constant care to spare the civilian population, civilians and civilian objects during hostilities involving cyber operations.[42]

Those who plan, approve or execute attacks must take **all feasible precautions in the choice of means and methods** with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects.[43] This might encompass **gathering intelligence on the network in question** through mapping or other processes in order to assess the attack's likely effects. Also, the **inclusion of a deactivation mechanism** or a specific configuration of the cyber tool which limits the effects on the intended target might be considered. Moreover, if it becomes apparent that the target is not a military one or is subject to special protection, those who plan, approve or execute the cyber attack must refrain from executing or suspend the attack. The same applies when the attack may be expected to cause excessive collateral damage to civilians and civilian objects.[44]

The obligation to take precautions in attack is complemented by the **obligation to conduct weapon reviews of any new means or method of cyber warfare** to determine whether its employment would, in some or in all circumstances, be prohibited by international law.[45] The findings of such reviews, to the extent that they identify legal constraints for the employment of means and methods in particular operational settings, should serve as a basis for operational planning. However, the means and methods used in cyber warfare are typically tailored to their targets, as they generally involve exploiting vulnerabilities that are specific to the target and the operational context. This entails that the development of means or the adoption of the method will often coincide with the planning of a concrete operation. Thus, the obligation to take precautions in attack and the requirement of a legal review remain separate requirements, but may overlap in substance.

IV. States' response options

a) Attribution

Attributing a cyber incident is of critical importance as a part of holding States responsible for wrongful behaviour and for documenting norm violations in cyberspace. It is also a prerequisite for certain types of responsive action. As regards the attribution of certain acts to States under international law, Germany applies the relevant **customary law rules on State responsibility also to acts in cyberspace,** subject to any *lex specialis* provisions. *Inter*

---

42 Additional Protocol I (note 35), art. 57 para. 1; Tallinn Manual 2.0 (note 4), rule 114.

43 Cf. Additional Protocol I (note 35), art. 57 para. 2 (a) (ii); Tallinn Manual 2.0 (note 4), rule 116.

44 Additional Protocol I (note 35), art. 57 para. 2 (a) (iii); art. 57 para. 2 (b); Tallinn Manual 2.0 (note 4), rules 117, 119.

45 In Germany, the legal review is carried out by the steering committee for the review of new weapons and methods of warfare under the direction of the Directorate-General for Legal Affairs, Joint service regulation A 2146/1.

alia, cyber operations conducted by **State organs** are attributable to the State in question.[46] The same applies with regard to **persons or entities which are empowered by the law of a State to exercise elements of the governmental authority** and act in that capacity in the particular instance.[47] Attribution is not excluded because such organ, person or entity acting in an official capacity exceeds its authority or contravenes instructions – cyber operations conducted ***ultra vires*** are likewise attributable to the State in question.[48] This applies *a maiore ad minus* when only parts of an operation are *ultra vires*.

Generally, the mere (remote) use of cyber infrastructure located in the territory of a State (forum State) by another State (acting State) for the implementation of malicious cyber operations by the latter does not lead to an attribution of the acting State's conduct to the forum State. However, the forum State may under certain circumstances incur responsibility on separate grounds, for example if its conduct with regard to another State's use of its cyber infrastructure for malicious purposes qualifies as **aid or assistance.**[49] This *inter alia* applies if the forum State actively and knowingly provides the acting State with access to its cyber infrastructure and thereby facilitates malicious cyber operations by the other State.[50]

Moreover, cyber operations conducted by **non-State actors which act on the instructions of, or under the direction or control of, a State** are attributable to that State.[51] The same principles apply as in the physical world: if a State recurs to private actors in order to commit an unlawful deed, the actions by the private actor will regularly be attributable to the State. States should recognize that they are accountable for the actions of proxies acting under their control.[52] The State must have control over a specific cyber operation or set of cyber operations conducted by the non-State actor. While a sufficient degree or intensity of such control is necessary, the State is **not required to have detailed insight into or influence over all particulars, especially those of a technical nature, of the cyber operation.** A comprehensive assessment of the circumstances of the individual case will be necessary to establish an attributive link.[53]

Beyond the mentioned situations of attribution and aid and assistance, a State may also become liable under international law in connection with another State's or a non-State actor's actions if the first State fails to abide by its obligations stemming from the 'due diligence' principle.[54]

---

46 Cf. International Law Commission (ILC), Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001, in: Report of the International Law Commission on the work of its fifty-third session, 23 April – 1 June and 2 July – 10 August 2001, Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 10, UN Doc. A/56/10, 26 *et seq.,* art. 4; Tallinn Manual 2.0 (note 4), rule 15.

47 Cf. Draft Articles on State Responsibility (note 46), art. 5; Tallinn Manual 2.0 (note 4), rule 15.

48 Cf. Draft Articles on State Responsibility (note 46), art. 7; Tallinn Manual 2.0 (note 4), rules 15, commentary, paras. 6, 12.

49 Cf. Draft Articles on State Responsibility (note 46), art. 16; Tallinn Manual 2.0 (note 4), rule 18 (a).

50 Cf. Draft Articles on State Responsibility (note 46), art. 16, commentary, para. 1; Tallinn Manual 2.0 (note 4), rule 18, commentary, para. 3.

51 Cf. Draft Articles on State Responsibility (note 46), art. 8; Tallinn Manual 2.0 (note 4), rule 17 (a).

52 Cf. UN Group of Governmental Experts, reports of 2013 and 2015 (note 1), paras. 23 and 28 (e) respectively.

53 Cf. Draft Articles on State Responsibility (note 46), art. 8, commentary, paras. 5 *in fine,* 7.

54 See also above, II.a).

The application of the international rules on State responsibility and hence the act of formally attributing a malicious cyber operation to a State under international law is first and foremost a national prerogative; however, international cooperation and exchange of information with partners in this regard can be of vital importance. In practice, establishing the facts upon which a decision on attribution may be based is of specific concern in the context of cyber operations since the author of a malicious cyber operation may be more difficult to trace than that of a kinetic operation. At the same time, **a sufficient level of confidence** for an attribution of wrongful acts needs to be reached. Gathering relevant information about the incident or campaign in question has a technical dimension and may involve processes of data forensics, open sources research, human intelligence and reliance upon other sources – including, where applicable, information and assessments by independent and credible non-state actors. Generating the necessary contextual knowledge, assessing a suspected actor's motivation for conducting malicious cyber operations and weighing the plausibility of alternative explanations regarding the authorship of a certain malicious cyber act will likewise be part of the process. All relevant information should be considered.[55]

Germany agrees that there is no general obligation under international law as it currently stands to publicize a decision on attribution and to provide or to submit for public scrutiny detailed evidence on which an attribution is based. This generally applies also if response measures are taken.[56] Any such publication in a particular case is generally based on political considerations and does not create legal obligations for the State under international law. Also, it is within the political discretion of a State to decide on the timing of a public act of attribution. Nevertheless, Germany supports the UN Group of Governmental Experts' position in its 2015 report that **accusations of cyber-related misconduct against a State *should* be substantiated.**[57] States should provide information and reasoning and – if circumstances permit – attempt to communicate and cooperate with the State in question to clarify the allegations raised. This may bolster the transparency, legitimacy and general acceptance of decisions on attribution and any response measures taken.[58]

Attribution in the context of State responsibility must be distinguished from politically assigning responsibility for an incident to States or non-State actors: Generally, such statements are made at the discretion of each State and constitute a manifestation of State sovereignty. Acts of politically assigning responsibility may occur in cooperation with partners. As regards attribution in the legal sense, findings of national law-based (court) proceedings involving acts of attribution, for example in the context of criminal liability of certain office holders or non-State actors, may serve as indicators in the process of establishing State responsibility. However, it should be borne in mind that the criteria of attribution under international law do not necessarily correspond to those under domestic

---

55 Cf. also the voluntary, non-binding recommendation made by the UN Group of Governmental Experts, report of 2015 (note 1), para. 13 (b).

56 On these points, see Tallinn Manual 2.0 (note 4), chapter 4, section 1, para. 13.

57 UN Group of Governmental Experts, report of 2015 (note 1), para. 28 (f).

58 Cf. also Tallinn Manual 2.0 (note 4), chapter 4, section 1, para. 13, citing the UN Group of Governmental Experts, report of 2015 (note 1).

law and that additional or specific criteria are generally relevant when establishing State responsibility for individually attributed conduct. Moreover, the adoption of targeted restrictive measures against natural or legal persons, entities or bodies under the EU Cyber Sanctions Regime[59] does not as such imply the attribution of conduct to a State by Germany in a legal sense.[60]

b) Measures of response

(1) Retorsion

A State may engage in measures of retorsion to counter a cyber operation carried out against it. Retorsions are unfriendly acts directed against the interests of another State without amounting to an infraction of obligations owed to that State under international law. Since retorsions are predominantly rooted in the political sphere, they are not subject to such stringent legal limitations as other types of response such as countermeasures.

Measures of retorsion may be adopted to **counter (merely) unfriendly cyber operations** perpetrated by another State. They may likewise be enacted in reaction to an unlawful cyber operation **if more intensive types of response (countermeasures, self-defence) are unavailable for legal reasons (for example, in cases in which counter-measures would be disproportionate) or politically unfeasible.** Moreover, they may be adopted as a reaction to an unlawful cyber operation **in combination with other types of response,** such as countermeasures, as part of a State's comprehensive, multi-pronged response to malicious cyber activities directed against it.

(2) Countermeasures

The law of countermeasures allows a State to react, under certain circumstances, to cyber-related breaches of obligations owed to it by another State by taking measures which for their part infringe upon legal obligations it owes to the other State.[61] If certain legal conditions are met, such measures do not constitute wrongful acts under the international law of State responsibility.[62] Germany agrees that **cyber-related as well as non-cyber-related breaches of international obligations may be responded to by both cyber and non-cyber countermeasures.[63]**

---

59 Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17 May 2019, p. 1–12; Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17 May 2019, p. 13–19, as last amended by Council Decision (CFSP) 2020/1748 of 20 November 2020, OJ L 393, 23 November 2020, p. 19-20.

60 Cf. also Council Decision (CFSP) 2019/797 of 17 May 2019 (note 59), recital 9.

61 Draft Articles on State Responsibility (note 46), part III, chapter II, introductory commentary; Tallinn Manual 2.0 (note 4), rule 20 (with the commentaries).

62 Draft Articles on State Responsibility (note 46), art. 22.

63 Tallinn Manual 2.0 (note 4), rule 20 (with the commentaries).

As regards the **limitations to countermeasures,** Germany is of the opinion that, **generally, the same conditions apply as in non-cyber-related contexts:** In particular, countermeasures may only be adopted against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations arising from its responsibility (in particular cessation of the wrongful act).[64] Also, they must be proportionate and respect fundamental human rights, obligations of a humanitarian character prohibiting reprisals and peremptory norms of international law.[65]

Due to the multifold and close interlinkage of cyber infrastructures not only across different States but also across different institutions and segments of society within States, cyber countermeasures are specifically prone to generating unwanted or even unlawful side effects. Against this background, States must be **particularly thorough and prudent in examining whether or not the applicable limitation criteria to cyber countermeasures are met.**[66]

A State may – *a maiore ad minus* – engage in cyber reconnaissance measures in order to explore options for countermeasures and assess the potential risk of side effects if such measures fulfil the requirements for countermeasures.

(3) Measures taken on the basis of necessity

The wrongfulness of a State's cyber operation that contravenes its international obligations may be precluded by exception if that State acted out of necessity.[67] This entails that a State may – under certain narrow circumstances – act against malicious cyber operations by resorting, for its part, to active counter-operations even in certain situations in which the prerequisites for countermeasures or self-defence are not met.

The draft articles on State responsibility, which reflect customary law in this regard, *inter alia* require that the act must be 'the only way for the State to safeguard an essential interest against a grave and imminent peril'.[68] Whether an 'interest' is 'essential' depends on the circumstances.[69] Germany holds the view that, in the cyber context, the affectedness of an 'essential interest' may *inter alia* be explained by reference to the **type of infrastructure actually or potentially targeted** by a malicious cyber operation and an analysis of that

64 Draft Articles on State Responsibility (note 46), art. 49 para. 1 (with the commentaries); Tallinn Manual 2.0 (note 4), rule 21.

65 Draft Articles on State Responsibility (note 46), arts. 51, 50 para. 1 (b), (c), and (d); cf. Tallinn Manual 2.0 (note 4), rules 23, 22.

66 Tallinn Manual 2.0 (note 4), rule 23, commentary, para. 6.

67 Cf. International Court of Justice (ICJ), Gabčíkovo-Nagymaros Project (Hungary v. Slovakia), Judgement of 25 September 1997, I.C.J. Reports 1997, 7, para. 51; Draft Articles on State Responsibility (note 46), art. 25; Tallinn Manual 2.0 (note 4), rule 26 with commentaries.

68 Draft Articles on State Responsibility (note 46), art. 25 para. 1 (a). The Draft articles on State Responsibility further require that the act in question must 'not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole' and state that 'necessity may [in any case] not be invoked by a State as a ground for precluding wrongfulness if: (a) the international obligation in question excludes the possibility of invoking necessity; or (b) the State has contributed to the situation of necessity', see art. 25 para. 1 (b) and 2.

69 Draft Articles on State Responsibility (note 46), art. 25, commentary, para. 15.

infrastructure's relevance for the State as a whole. For example, the protection of certain critical infrastructures[70] may constitute an 'essential interest'.[71] It might likewise be determined by reference to the ***type* of harm actually or potentially caused** as a consequence of a foreign State's cyber operation. For example, the protection of its citizens against serious physical harm will be an 'essential interest' of each State – regardless of whether a critical infrastructure is targeted or not. Nevertheless, given the exceptional character of the necessity argument, an 'essential interest' must not be assumed prematurely.

A case-by-case assessment is necessary to determine whether a peril is 'grave'. The more important an 'essential interest' is for the basic functioning of a State, the lower the threshold of the 'gravity' criterion should be. Germany agrees that a **'grave peril' does not presuppose the occurrence of physical injury** but may also be caused by large-scale functional impairments.[72]

A State, when confronted with a cyber threat, **does not yet need to have assessed the *total* and *final* damage potential in order to invoke necessity.**[73] Necessity may be invoked when the origin of a cyber measure has not (yet) been clearly established;[74] however, States should always make efforts to clarify attribution and (State) responsibility in order to be able to substantiate their grounds for action.

(4) Self-defence

The right to self-defence according to art. 51 UN Charter is triggered if an armed attack occurs. Malicious cyber operations can constitute an armed attack whenever they are **comparable to traditional kinetic armed attack in scale and effect.** Germany concurs with the view expressed in rule 71 of the Tallinn Manual 2.0.

Furthermore, Germany acknowledges the view expressed in the ICJ's Nicaragua judgment, namely that an armed attack constitutes the gravest form of use of force.[75] Assessing whether the scale and effects of the cyber operation are grave enough to consider it an armed attack is a political decision taken in the framework of international law. **Physical destruction of property, injury and death (including as an indirect effect) and serious territorial incursions are relevant factors.** The decision is not made based only on technical information, but also after assessing the strategic context and the effect of the cyber

---

70 On the concept of 'critical infrastructures' see above, II.a).

71 Tallinn Manual 2.0 (note 4), rule 26, commentary, para. 2, correctly noting, however, that the 'designation [of an infrastructure as critical by a State] as such does not necessarily deprive other infrastructure of its essentiality' and that 'a State's unilateral description of infrastructure as critical [is not] determinative of the issue.'

72 Tallinn Manual 2.0 (note 4), rule 26, commentary, para. 4.

73 Cf. Draft Articles on State Responsibility (note 46), art. 25, commentary, para. 16: '[...] a measure of uncertainty about the future does not necessarily disqualify a State from invoking necessity, if the peril is clearly established on the basis of the evidence reasonably available at the time.'

74 Tallinn Manual 2.0 (note 4), rule 26, commentary, para. 11. Reasonableness standards apply to *ex ante* determinations depending on the context; see also Tallinn Manual 2.0 (note 4), Chapter 4, Introduction to Section 1, para. 9-11.

75 ICJ, Military and Paramilitary Activities in and against Nicaragua (note 21), para. 191.

operation beyond cyberspace. This decision is not left to the discretion of the State victim of such a malicious cyber operation, but needs to be comprehensibly reported to the international community, i.e. the UN Security Council, according to art. 51 UN Charter.

The response to malicious cyber operations constituting an armed attack is not limited to cyber counter-operations. Once the right to self-defence is triggered, the State under attack **can resort to all necessary and proportionate means in order to end the attack.** Self-defence does not require using the same means as the attack which provided the trigger for its exercise.

Acts of non-State actors can also constitute armed attacks. Germany has expressed this view both with regard to the attacks by Al Qaeda[76] and the attacks of ISIS.[77]

In Germany's view, art. 51 UN Charter requires the attack against which a State can resort to self-defence to be 'imminent'. The same applies with regard to self-defence against malicious cyber operations. Strikes against a prospective attacker who has not yet initiated an attack do not qualify as lawful self-defence.

V. Conclusions and outlook

As has been exemplified in the present paper with regard to a selection of international norms, international law as it stands is capable of providing essential guidance on State behaviour in and with regard to cyberspace. Germany is convinced that **uncertainties as to how international law might be applied in the cyber context can and must be addressed by having recourse to the established methods of interpretation of international law.**[78] Germany deems it critically important that interpretative efforts and attempts to clarify the modalities of the application of international law in cyberspace are based on international exchange and cooperation. This is why Germany follows closely and is actively involved in the work of the **United Nations' working groups on cyber and international security.**[79] In addition to their work on international law in cyberspace, these groups elaborate voluntary, non-binding norms for responsible State behaviour in cyberspace which may fulfil an important function in supplementing the existing 'hard' rules of international law. Moreover, Germany wishes to highlight the importance of States' reflecting and taking heed of the multifold and rich **academic and civil society debates** worldwide on the role and function of international law in the cyber context.

---

76 See Letter dated 29 November 2001 from the Permanent Representative of Germany to the United Nations addressed to the President of the Security Council, UN Doc. S/2001/1127.

77 See Letter dated 10 December 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations addressed to the President of the Security Council, UN Doc. S /2015/946.

78 In the case of international treaties, these are codified in arts. 31 *et seq.* of the Vienna Convention on the Law of Treaties, 23 May 1969, UNTS 1155, 331.

79 I.e. the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) and the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG).

Challenges lie ahead: Information and communication technologies are evolving fast, and so is the need to provide adequate legal assessments and to find responses to novel factual situations. While international law provides a sufficient framework to cope with the fast pace of technological change and remains applicable also to new developments, its interpretation and effective application in the cyber context will increasingly be dependent on an in-depth understanding of technological intricacies and complexities. This may require an **intensified pooling of technical and legal expertise.** Also, evidentiary difficulties with regard to States' and non-State actors' behaviour in cyberspace will continue to pose practical challenges. Nevertheless, while underlining the prime responsibility of States for maintaining peaceful relations and upholding the rule of law in the international system, Germany is convinced that the **combined efforts of States, international organizations, civil society and academia will continue to provide significant insights into the modalities of how international law applies in the cyber context,** thereby leading to a high standard of international legal certainty with regard to this still relatively novel dimension of international relations.