***Delerue, François*: Cyber Operations and International Law.** Cambridge: Cambridge University Press, 2020. ISBN 978-1-108-49027-6 (Hardback). xviii, 522 pp. £ 120.-; eISBN 978-1-108-80117-1, US$ 36.-

How well can international law (IL) adapt to cyberspace? Are existing norms of IL sufficiently flexible to regulate a borderless, non-physical domain that has been created and increasingly conquered only recently? '*Cyber Operations and International Law*' sets out on the ambitious task to answer these questions. The book by *François Delerue* provides an analysis of the strengths and weaknesses of a legal order facing unprecedented challenges – from cyber-attacks on nuclear plants to election meddling through digital espionage.

The result of *Delerue's* analysis is a comprehensive study of the current state of IL applicable to cyber operations; in its length, depth, and thoroughness one of the first of its kind. Taking the classic law of state responsibility as his starting point and foundation, the author meticulously lays out the international legal framework limiting states' behaviour in cyberspace. The book will not only appeal to international legal scholars however. *Delerue* makes an effort to bridge the gap between lawyers, computer- and political scientists, explaining the essentials of each discipline to the others where necessary. The author would be well-positioned to embark on that endeavour, researching at the intersection of cybersecurity and law, and – as the special rapporteur on international law of the EU Cyber Direct Project – close to practice.

The structure of the book follows the one of the Articles on State Responsibility (ASR). The criteria to establish a cyber operation's attribution to a state (Part I), its (un-)lawfulness (Part II), and the remedies a victim state has at its disposal (Part III) are laid out successively. In its outline, the book thus recalls the structure of a commentary one may take to hand in examining a real-world case of a state-sponsored cyber operation. In its analysis however, the compendium goes beyond a mere description or extraction of the *lex lata* applicable to states' behaviour in cyberspace.

Indeed, *Delerue's* aspiration to contribute substantially to the discussion surrounding the immense challenges regarding the application of IL to cyber operations becomes clear already in his introductory chapter. Rightly so, he criticises what he perceives as a discussion held in reverse, putting the cart before the horse: That IL is applicable to cyber operations, he suggests, cannot be the start of the journey. The latter is instead a claim to be proven, ideally via analysing *how* it is applicable, via identifying gaps and insufficiencies of traditional IL on the way. Only in that manner, the (in-)necessity of a new treaty or new rules tailored specifically to cyberspace becomes evident.

DOI 10.17104/0044-2348-2021-3-879

https://doi.org/10.17104/0044-2348-2021-3-879 - am 28.01.2026, 16:39:05. https://www.inlibra.com/de/agb - Open Access -

That '*[n]othing prevents international law from applying to cyberspace*' (p. 6) will thus be – one of the many – outcomes of his book. Certainly, this approach requires a close examination of classic IL. The more advanced reader may therefore be surprised to find rather lengthy sections of the book without any reference to modern technologies whatsoever. A closer intertwinement of these parts with the cyber context might at times have indeed been desirable. Then again, it is the compendium's solid doctrinal foundation that makes out one of its major achievements.

Delerue completes his introductory thoughts with a comparison of cyberspace to other areas of human life whose regulation through IL was formerly contested as well. The side view on international air and space law, however, serves mainly to carve out a major difference hereto: cyberspace, it is argued, is not a new physical environment. It is instead part of the domains of land, sea, air, and space already regulated by IL.

These meta-considerations regarding the nature of cyberspace are subsequently contrasted by an overview of some of the practical challenges still affecting that very same application process: Most prominently, the 2017 failure of the United Nations Group of Governmental Experts (UNGGE) to formally agree upon draft paragraph 34 of its final report. Therein, the experts had planned to assert the general applicability of IL to the state use of information and communication technologies.

It is at this point where the author's view on IL's potential and limits in cyberspace shines through for the first time. That he perceives the failure not as such but rather as '*a demonstration of the vigorous academic and international discussion of these matters*' (p. 15) might at first sight seem overly optimistic. *Delerue* however applies a sober and realist approach in his assertations, drawing on established techniques of interpretation and guiding principles of IL. He is not hesitant to highlight the risk of a geographical fragmentation of IL due to the rejection of paragraph 34 by certain states. On the other hand, he equally elaborates on how the '*significance of that attitude is to confirm rather than to weaken the rule*' (p. 18).

Drawing on the existing law of state relations, most impressively by consulting a vast array of international jurisprudence, is one of the techniques that will give the most credibility to the author's line of argument. This becomes clear from the start of the main part of the book, analysing in a first step the attribution of cyber operations to states (Part I). A such may be attributed directly to the latter, to an individual, or else to the machine the operation is launched from. These three dimensions need to be perceived as separate from one another, particularly due to the numerous technical possibilities of hiding the true location or identity of the computer. The author gives an overview of the technical forensics at stake, comprehensible also for

 DOI 10.17104/0044-2348-2021-3-879

https://doi.org/10.17104/0044-2348-2021-3-879 - am 28.01.2026, 16:39:05. https://www.inlibra.com/de/agb - Open Access -

those unfamiliar with the relevant details of applied informatics. It becomes clear how very easily serial numbers, IP and MAC addresses can be '*spoofed*' (p. 67).

This risk of misidentification, linked to the technical challenges of the process of attribution, is however but one side of the coin. Its practical challenges further relate to (geo-)political pitfalls: Which state would be keen to publish technical evidence on an adversary's cyber-attack, revealing in this way its very own computing capabilities – and vulnerabilities? Particular legal challenges will often emerge where non-state actors come into play. As so often, *Delerue* works with hypothetical and real-world examples to make his point on this issue, a key aspect of his analysis. Painting the picture of Distributed Denial of Service (DDoS) attacks on crucial infrastructure, he explains how with a low degree of organisation, individuals working together have a formerly unknown power in cyberspace. Where states incite private persons to act *en masse* in such a way, the often extremely low level of control they may exercise over their 'helpers' will cause trouble in attributing their acts to the state. To come to this conclusion, *Delerue* goes into detail regarding the highly ambiguous jurisprudence on the attribution of acts of non-state actors to states. In this way, a classic of the debate surrounding the jurisprudential fragmentation of IL attaints a surprisingly new significance in the cyber context. Having made proof in his introductory chapter of being aware of this discussion, some readers may, however, be left partially unsatisfied by the author's handling of it. For once, relevant judgements are enumerated without explicitly explaining their conjunct standing as *the* prime example of fragmentation in IL. Not only the non-lawyer equally addressed by the book may be left fairly puzzled by the different judicial responses to the same problem. That the subsequent debate on these verdicts indeed produced ways to flatten contradictions between them could therefore have been made clearer. The position, for instance, that the International Tribunal for the Former Yugoslavia delivered a judgement *ultra vires* by treating questions of state responsibility might have been worthwhile considering.

In Part II, the author moves on to an analysis of the nature and lawfulness of cyber operations. While underlining how these are not explicitly prohibited under IL, multiple ways in which they may still breach its primary rules are examined. The main outcome of this section goes hand in hand with *Delerue's* intention to contribute to filling a gap in the existing literature. Indeed, scholarship has long focused on the extreme scenario of cyber warfare. Cases, however, in which cyber operations cross the threshold of the use of force or an armed attack, in the latter event even triggering the right to self-defence of a victim state, are rare.

https://doi.org/10.17104/0044-2348-2021-3-879 - am 28.01.2026, 16:39:05. https://www.inlibra.com/de/agb - Open Access -

Going beyond '*the tip of the iceberg*' (p. 44), the book therefore gives special attention to infringements of IL beneath the threshold. Naturally, this includes first establishing where that (highly controversial) line is drawn in cyberspace. Presenting the different approaches elaborated by scholars to this end, *Delerue* himself stands closest to a consequences-based criterion: the nature of the target affected by a cyber operation as well as the type of damage caused to it are to be considered. In line with the position held by the *Tallinn Manuals* and a seeming majority of scholars, it is therefore argued that physical damage cannot be the only factor in assessing questions of cyber force. Where (non-physical) data, stored for instance in a critical industrial facility, is erased, this could also amount to such a use of force.

Where the threshold is not met, in turn, the cyber operation may still have breached the territorial sovereignty of a state or could constitute a violation of the principle of non-intervention. On the latter, *Delerue* appears to again argue in line with the majoritarian view, holding that the intervention must be coercive. Laying an important focus on questions surrounding the interferences in the American and French elections in 2016 and 2017, the respective section ends with a strong empirical analysis – and a daring conclusion. Unlike others, *Delerue* sees coercion in the above cases at least where data taken through hacks was released to the public. His taking on when a state's sovereignty is violated by a cyber operation, is equally worth a read. Pointing towards how the passing of a ship through a state's territorial waters may amount to a violation of the latter's sovereignty in traditional IL, he convincingly criticises how the *Tallinn Manual* requires a certain harm to result from a 'cyber passing'.

Temporarily departing from the structure of the ASR, potential violations of human rights (HR) and, at the lowest end of the intensity-scale, of the principle of due diligence are equally discussed. This step outside the line, however, is very much justified. At least the field of HR constitutes a crucial example for areas in which IL might have to openly deviate from established standards to satisfyingly regulate cyber operations. Having 'effective control' over an individual abroad might be too strict of a standard to ensure respect for fundamental rights in the cyber context. Similarly, states might abuse of the principle of due diligence by taking it as an excuse to justify mass surveillance programmes – an approach that would erode the principle's very basis.

Lastly, Part III of *Delerue's* work explores the remedies the targeted state of a cyber operation has at hand to invoke the attacking states' responsibility under IL. The usual suspects apply: Where a request for cessation and/or for reparation is not met, the state may resort to measures of self-help. The specificities of cyber operations will make some of these more or less likely to provide assistance: Where data is erased, it cannot be brought back

 DOI 10.17104/0044-2348-2021-3-879

https://doi.org/10.17104/0044-2348-2021-3-879 - am 28.01.2026, 16:39:05. https://www.inlibra.com/de/agb - Open Access -

through restitution. Where a cyber-attack lasts only a fraction of a second, demanding cessation will be superfluous.

In line with the author's finding that cyber operations below the threshold of an armed attack are to be given more attention, he underlines how countermeasures – not self-defence – will be the '*primary and preferred*' form of self-help in the cyber realm (p. 424). Their aim must be to compel the wrongdoing state to comply with its obligation, commonly applying measures with merely reversible effects. *Delerue* approves of voices in the literature pointing towards the downsides of this limitation in the cyber realm. Unlike acts of self-defence, moreover, these measures may only be taken individually by the affected state. Vast gaps in terms of cyber-warfare capabilities will do the rest, impeding a targeted David to efficiently act against a Goliath, leading *Delerue* to make out these limitations as a major deficiency of IL in cyberspace. Unfortunately, the author avoids too large of a discussion on *erga omnes* norms in this context. These overarching obligations that not only allow but even oblige all states to react in cases of violation would, according to *Delerue*, be unlikely to be affected by cyber operations. The reader might wonder, however, why the vast power that can be exercised through digital means – and that becomes evident throughout the book – could not equally be used one day to commit violations legally affecting all states.

The author's overall answer to how well he sees IL prepared to accommodate the challenges of cyberspace is thus a split one. Where he identifies legal gaps, he takes them seriously, recommending to establish more suitable frameworks. He speaks out for renewed standards on human rights in cyber space, makes a forward-thinking suggestion on a potential duty to prevent transboundary harm caused by cyber operations and seems to find a tailor-made new approach to cyber force appealing. Needless to say, the highly diverging – indeed fragmented – opinions of states on these issues render a treaty on these topics a rather distant prospect.

Incidentally, this is equally the case for autonomous cyber operations, an issue virtually neglected in the literature besides its more appealing older sister of lethal autonomous weapon systems (LAWS). In line with his – highly justified – criticism that cyber warfare is generally given too much attention compared to its practical importance, *Delerue* finds autonomous cyber operations a crucial topic not to be forgotten. However, one is surprised in view of how rather unproblematic he perceives their actions' attribution to a state to be. Where programmed and launched by one, there should be no question, he argues. While certainly a tenable position, a more in-depth examination of the opposing voices in the context of LAWS might have given his argument more stability at that point.

DOI 10.17104/0044-2348-2021-3-879

https://doi.org/10.17104/0044-2348-2021-3-879 - am 28.01.2026, 16:39:05. https://www.inlibra.com/de/agb - Open Access -

More generally, the reader of the presented volume might occasionally question how specific to the cyber context some of the gaps identified actually are. At least on the topic of countermeasures, one must admit that differences in warfare capabilities and such measures being uniquely permitted to the targeted state alone have posed problems in traditional scenarios as well. Nonetheless, *Delerue* aptly achieves to show how cyberspace serves as a burning glass under which these issues – that have long exposed IL to criticism – are now emerging clearer than ever. The topic of attribution of acts of non-state actors comes to mind in this context, a question that has remained unanswered for too long and whose consequences will unquestionably pose even more prominent perils in the cyber future. The same goes for equally contested topics such as the one of anticipatory self-defence. Unsettled questions will become more pressing in times where split seconds might count in repelling a cyber-attack.

The IL gaps he identifies aside, the true value of *Delerue's* work might be found elsewhere. In times where the international legal order itself is under constant attack, his assertation that nonetheless '*international law matters in cyberspace*' is an important one (p. 495). In this context, an aspect a review of his work cannot forego needs mentioning: his substantial, albeit critical, evaluation of the *Tallinn Manual 2.0*. In his book, *Delerue* draws on the expert manual with caution, unhesitant to criticise its authors' conclusions. That he would take the manual not as an authority set in stone but as a work marked by compromise allows him to come to some stimulating conclusions. Most importantly, nothing but his own analysis of the current state of IL is taken as the foundation of his chapters – not the manual claiming to have already laid out the same. Consequently, he uncovers instances where *Tallinn 2.0* deviates from what he convincingly, after thorough and in-depth evaluation of state practice and jurisprudence, identifies as the *lex lata* (see particularly pp. 198, 217, 363). The solution will not always be as simple as applying the existing law as it is. Nonetheless, at least not complicating matters unnecessarily appears a good way to start.

Rachel F. Behring, Berlin

 DOI 10.17104/0044-2348-2021-3-879

https://doi.org/10.17104/0044-2348-2021-3-879 - am 28.01.2026, 16:39:05. https://www.inlibra.com/de/agb - Open Access -

EU-Grundrechte auf neuestem Stand.

Der »Jarass«

kommentiert die mit dem Vertrag von Lissabon rechtsverbindlich erklärte Grundrechte-Charta und bietet zudem einen einführenden Überblick über das System des Europäischen Grundrechtsschutzes.

Wichtig für deutsche Juristen

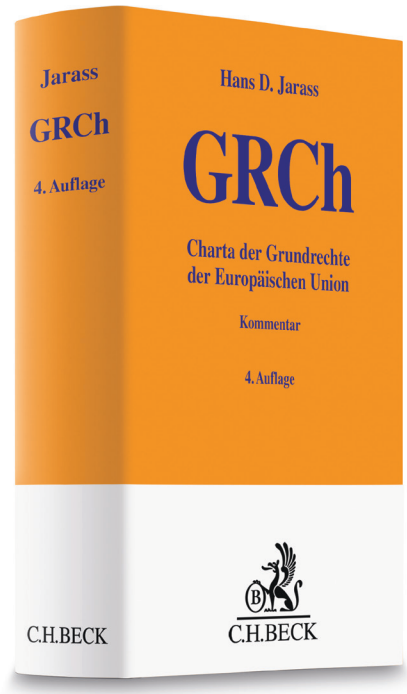
Die europäischen Grundrechte sind nicht deckungsgleich mit den deutschen Grundrechtsregelungen. Teilweise werden Schutzbereiche normiert, die im Grundgesetz nicht ausdrücklich geregelt sind, wie z.B.

- der Schutz persönlicher Daten
- das Recht auf Bildung
- Rechte von Kindern und Älteren
- die Gewährleistungen zum individuellen Arbeitsrecht oder
- das Recht auf eine gute Verwaltung.

Die 4. Auflage

verarbeitet die seit der Vorauflage ergangene Rechtsprechung des EuGH (und des EuG) und der nationalen Gerichte sowie die umfangreiche neue Literatur.

Rechnung getragen wurde insbes. der gestiegenen Bedeutung der Rechtsschutzgewährleistung in Art. 47, auch für Verfahren vor den nationalen Gerichten.



Jarass
GRCh · Charta der Grundrechte der Europäischen Union

4. Auflage. 2021. XV, 572 Seiten.
In Leinen € 119,–
ISBN 978-3-406-76314-4

beck-shop.de/31693719

Der Autor

Professor Dr. Hans D. **Jarass** ist einer der bekanntesten Staatsrechtslehrer im deutschsprachigen Raum. Auf dem Gebiet des Verfassungsrechts ist er insbesondere durch seinen Standardkommentar zum Grundgesetz der Bundesrepublik Deutschland, der im Jahr 2020 unter Mitwirkung von Prof. Dr. Martin Kment in 16. Auflage erschienen ist, hervorgetreten.

”

... eine hervorragende Praxishilfe, die nicht zuletzt auch einer ersten Einarbeitung in die - auch manchem grundrechtsgeschulten deutschen Juristen eher noch fremde – Materie des Grundrechtsschutzes auf EU-Ebene dienen kann.

Prof. Dr. Hermann Weber, in: LKV 03/2017, zur 3. Auflage 2016

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 172622
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK

https://doi.org/10.17104/0044-2348-2021-3-679 - am 28.01.2026, 16:39:05. https://www.inlibra.com/de/agb - Open Access -

Handbuch Ius Publicum Europaeum

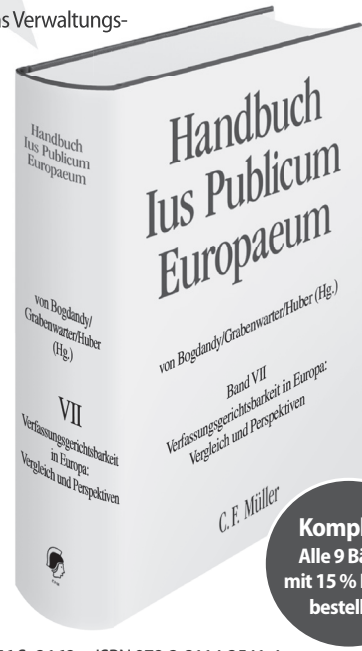
Band VII: Verfassungsgerichtsbarkeit in Europa: Vergleich und Perspektiven

Herausgegeben von Prof. Dr. Armin von Bogdandy, MPI für ausländisches öffentliches Recht und Völkerrecht, Heidelberg, Prof. DDr. Christoph Grabenwarter, Wirtschaftsuniversität Wien, und Richter des BVerfG Prof. Dr. Peter M. Huber, Lehrstuhl für Öffentliches Recht und Staatsphilosophie, LMU München.

2021. X, 893 S. Geb. Buckram-Leinen mit Goldprägung. Mit Schutzumschlag. € 234,–. ISBN 978-3-8114-5315-9

Mit Beiträgen *von Armin von Bogdandy, Monica Claes, Anuscheh Farahat, Christoph Grabenwarter, Constance Grewe, Rainer Grote, Peter M. Huber, András Jakab, Christoph Krenn, Christine Landfried, José Martín y Pérez de Nanclares, Davide Paris, Juan Luis Requejo Pagés, Markus Vašek, Pedro Cruz Villalón, Maartje de Visser, Bruno de Witte.*

Die Edition „Ius Publicum Europaeum" behandelt das Verfassungs- und das Verwaltungsrecht im Lichte des gemeinsamen europäischen Rechtsraums. Dargestellt werden die Grundstrukturen der nationalen Verfassungen und deren Wissenschaft in repräsentativ ausgewählten Mitgliedstaaten der Europäischen Union. Die **Idee dieses Handbuchs** ist es, die unter dem Einfluss des europäischen Rechts stehenden nationalen Rechtsordnungen einer **rechtsvergleichenden Analyse** zu unterziehen und dabei Gemeinsamkeiten und Unterschiede aufzuzeigen. Die Landesberichte sind nach einheitlichen Kriterien erstellt und erläutern die nationalen Grundlagen, wodurch die Rechtsordnungen der einzelnen Staaten sehr gut miteinander vergleichbar sind.



Band VII vergleicht die **europäische Verfassungsgerichtsbarkeit** in der Perspektive des europäischen Rechtsraums. Er untersucht die Strukturen der Organisation, der Richterernennung, der Verfahren und der Argumentations- und Auslegungsmethoden, ihr Wirken in Staat und Gesellschaft, ihre Legitimität oder ihre Rolle in der Gewaltengliederung und komplettiert damit das Bild nach den Länderberichten in Band VI.

Komplett: Alle 9 Bände mit 15 % Rabatt bestellen!

Bereits erschienen (Band IX erscheint in Kürze):

Band I: Grundlagen und Grundzüge staatlichen Verfassungsrechts. 2007. VIII, 856 S. € 168,–. ISBN 978-3-8114-3541-4
Band II: Offene Staatlichkeit – Wissenschaft vom Verfassungsrecht. 2008. X, 970 S. € 198,–. ISBN 978-3-8114-6301-1
Band III: Verwaltungsrecht in Europa: Grundlagen. 2010. X, 636 S. € 148,–. ISBN 978-3-8114-9808-2
Band IV: Verwaltungsrecht in Europa: Wissenschaft. 2011. IX, 633 S. € 148,–. ISBN 978-3-8114-4144-6
Band V: Verwaltungsrecht in Europa: Grundzüge. 2014. X, 1.269 S. € 259,99. ISBN 978-3-8114-5506-1
Band VI: Verfassungsgerichtsbarkeit in Europa: Institutionen. 2016. X, 945 S. € 228,–. ISBN 978-3-8114-6006-5
Band VIII: Verwaltungsgerichtsbarkeit in Europa: Institutionen und Verfahren. 2019. X, 940 S. € 234,–. ISBN 978-3-8114-6757-6
Band IX: Verwaltungsgerichtsbarkeit in Europa: Gemeineuropäische Perspektiven und supranationaler Rechtsschutz. 2021. Ca. X, 1.050 S. Ca. € 250,–. ISBN 978-3-8114-4438-6

Alle 9 Bände mit 15% Rabatt: Ca. € 1.588,–. ISBN 978-3-8114-4114-9
Auch als E-Book-Ausgabe erhältlich! (ISBN 978-3-8114-9576-0)

C.F. Müller GmbH, Waldhofer Str. 100, 69123 Heidelberg, kundenservice@cfmueller.de
Bestellen Sie alle C.F. Müller-Titel jetzt bei: www.otto-schmidt.de.

C.F. Müller
CFM

© drubig-photo „Bundesverwaltungsgericht1" - Adobe Stock & © J. C. András: „Griechische Heldensagen für die Jugend bearbeitet" - Wikimedia Commons, gemeinfrei

https://doi.org/10.17104/0044-2348-2021-3-579 - am 28.01.2026, 16:39:05. https://www.inlibra.com/de/agb - Open Access -