BUSTED! THE TRUTH ABOUT THE 50 MOST COMMON INTERNET MYTHS

with summaries in German, Arabic, Chinese, French, Russian and Spanish

edited by
Matthias C. Kettemann and Stephan Dreyer
Leibniz Institute for Media Research |
Hansâ€‘Bredow-Institut

internetmythen.de • internetmyths.eu

Internet Governance Forum Berlin

25–29 November 2019

IGF BERLIN
2019

TABLE OF CONTENTS

Chapter I: Rights and Rules

Chapter II: Security and Safety

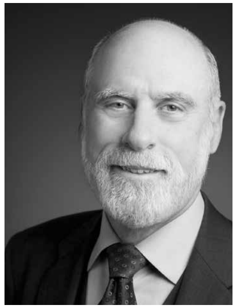
Chapter III: Inclusion and Integration

Chapter IV: Infrastructure and Innovation

Chapter V: Data and Disruption

At the Leibniz Institute for Media Research | Hans-Bredow-Institut, the authors would like to express their thanks to Wolfgang Schulz, Uwe Hasebrink, Kristina Hein, Jana Lemke, Katharina Mosene, Anna Sophie Tiedeke, Glacier Kwong, Jan Reschke, Johannes Schmees, Johanna Friederike Stelling, Johanna Sebauer and Ilse Kettemann.

PREFACE BY VINT G. CERF



Vinton G. Cerf, widely considered one of "the fathers of the Internet", is VP and Chief Internet Evangelist at Google. He helped found ICANN and was Chairman of its Board from 2000 to 2007. The recipient of many honorary degrees he has been awarded, inter alia, the National Medal of Technology, the Turing Award and the Presidential Medal of Freedom.

This is a wide-ranging compilation of opinions about the Internet and various truths and myths about its operation, use and impact. While I don't agree with all of the characterizations found in this collection, I think it is important to examine assertions made about the Internet and its applications both to clarify misunderstandings and to understand how some of these misrepresentations come about. Some originate in a kind of zealous hubris about the independence of cyberspace, which, on closer inspection, is revealed to be more bound to the physical and political world than one might think. Others strike me as excuses for adopting positions that are inimical to the beneficial uses of the present day Internet. What is important is for readers to approach these analyses in the spirit of ascertaining useful truths about the complex artifact that the Internet has become. The implementation and use of the Internet varies significantly from one jurisdiction to another, depending on physical infrastructure, culture, societal norms and available technology. The "myths" need to be examined and evaluated in context to be understood and properly evaluated.

My own biases are sure to be evident owing to my long-time involvement in many aspects of the Internet's creation and evolution, but I continue to believe that, as a platform, it has and will continue to be an extraordinary source of information, innovation and collaboration. The World Wide Web that rides atop the Internet infrastructure has promoted a cornucopia of applications and information infusion comparable to the invention of the printing press. But the unique flexibility of the underlying computing infrastructure provides a universe of functionality unreachable in the static print form. Content can be searched, translated, organized, repurposed, and adapted in ways limited only by our ability to imagine and write software to implement new capabilities.

The profusion of information found in the Net puts a burden on users to think critically about the quality, accuracy and veracity they find. This takes work and, in some sense, is the price we pay for the information freedom found in the online world. Those freedoms are at risk, however, precisely because the borderless Internet is more embedded in the political landscape than its enthusiastic promoters sometimes wish. Dispelling myths has the benefit of placing a reality lens on this remarkable environment and the resulting clarity can help us to steer a course towards an Internet whose benefits can consistently outpace its deficits.

PREFACE BY WOLFGANG SCHULZ

Wolfgang Schulz is Director, Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI), Hamburg; Chair of Media Law and Public Law including their Theoretical Foundations, University of Hamburg, holder of the UNESCO Chair for Freedom of Communication and Information, University of Hamburg; Director, Humboldt Institute for Internet and Society (HIIG), Berlin.

In this complex digital world, we – citizens, politicians and business leaders – need images and narratives that help us understand the world we live in. In most cases it is quite enough for us that these are plausible. We often cannot check whether they are true, and so the conclusiveness of a nice analogy or the fascination with a concept that brings complex developments down to earth is enough for us.

The echo chamber, one of the myths described in this book, can serve as an example. It has almost become a catchphrase to say that "we all live in echo chambers" at the opening of conferences. While this sounds plausible, it has only one small flaw – it's not true, at least not in this broad sense. It has been demonstrated that – at least in Germany where the "echo chamber" narrative is very popular – real echo chambers only exist for smaller extremist groups, not for society at large. Most people still want to be part of an overall "societal discourse" and use a broad media repertoire to gather information.

For the Internet, the services and the social practices that the Internet makes possible, this dependence on conclusive descriptions, metaphors and explanations is particularly strong. The Internet is not tangible, communications over networks are ultimately based on protocol standards. Nothing could be more abstract and yet its factual transformative power could hardly be greater, for better or for worse. Here, we are particularly dependent on images and narratives to orient ourselves in this realm, but also to find appropriate governance concepts.

Everyone who works with these metaphors, images and narratives has a great responsibility here. This is also and especially true for academia. It is not enough to carry out individual studies that refute the thesis of echo chambers and offer more sophisticated concepts. These concepts must also be conveyable in such a way that they can be connected to social discourse. Otherwise, the established myth will remain, even if some scholars know that it is empirically wrong. The authors and editors of this book deserve our sincere thanks – not only for drawing attention to this challenge, but also for starting to solve it right away.

INTRODUCTION BY THE EDITORS

The Moon landing was a fake. The Earth is flat. Vaccines are bad. These are myths you encounter on the Internet. But these are not Internet myths as we understand them – and debunk them – in this book; we rather bust Internet-related myths. In doing so, we rely on a broad conception of myth as coined by the influential French cultural theorist Roland Barthes: a myth is a cultural construction that appears to consist of universal truths embedded in common sense.

It is a myth, for instance, that what people do on the Internet cannot be regulated. It is a myth that protocols do not have politics. These powerful constructions of reality mystify the actual challenges in regulating the Internet. While containing some truth (it is often more difficult to regulate online behaviour than offline activities, and protocols have fewer "politics" than laws, which are distilled politics), they obfuscate what is actually at stake. This is the very reason that there are forces within the Internet policy field that have a vested interest in promulgating myths. The monsters of bad policy lurk in the shadows of myths about the way the Internet is being run. They feast and grow on disinformation, misinformation and the uncritical belief in stories we tell ourselves to make sense of the world(s) we construct for ourselves to make sense of the space we inhabit.

Psychologically, myths are attractive because they seem intuitive. Myths sound like helpful simplifications in ever more complex times. They suggest that we can stop reflecting, stop questioning the status quo, stop thinking of how to improve what we perceive. If algorithms are always neutral, then we do not need to develop normative tools to hold the companies accountable that develop and deploy them. Not thinking, not questioning, not looking at detail is always easier than the opposite.

Myths are seductive. Cybercriminals go free sounds like something we may have read, something that we may have heard even politicians say. But do they? Or does the myth hide the uncomfortable truth that they do not and that it takes hard forensically sound policing to counter them, rather than political posturing?

If search engines provide objective results, then there is no pressing need to open up a societal discourse on the duties of those structuring information. If privacy is dead, then why get riled up about privacy violations? If algorithms are neutral, then biases are an issue of the past.

But all isn't well in the state of the Internet (which, of course, isn't a state by itself: that laws do not apply online is a powerful myth in its own right).

Myths are like heuristics to help simplify the world. Like many heuristics myths may be useful, partially true or even be based on or encompass dearly held beliefs. In terms of economy of thought myths may make sense individually. Thinking is hard, critical thinking even more so. But societally, myths are very dangerous.

Many who use myths do so consciously. "Myth has the task", as Barthes wrote, "of giving a historical intention a natural justification and making contingency appear eternal". But each normative solution to a specific problem of Internet politics, policy and the global Internet polity is highly contingent. If we mystify the origins of the Internet, the role of algorithms, the character of code, the normativity of rules, the pluralism in cultures and concepts of life, we lose track of historical contingencies, cultural dependencies, the conditions of social interrelationships.

It is against this background that we decided to publish a call for Internet-related myths. We collected submissions and in a peer-reviewed process selected the 50 most representative ones. We are fully aware that the myths in this book only represent a fraction of the myths present in Internet governance discourses, but, we submit, it is a rather representative fraction that does cover many of the key themes and all of the broad thematic issues of the Internet Governance Forum in Berlin 2019, the occasion at which this book is published (the IGF is not just a talking shop, as another myth we demystify may want to have you believe).

Indeed, it was with a view to demystification of Internet governance discourses that we sought the cooperation of this year's host of the Internet Governance Forum 2019 in Berlin, whose financial support for this project is gratefully acknowledged. The responsibility for the selection and busting of the myths in this book, however, remains ours.

It is a responsibility we bear with great joy because we are convinced that the stellar team of authors from founders of the Internet to emerging scholars, from practitioners and professors to theorists and technologists, does a spectacular job in demystifying the Internet. Our goal was to provide a vade mecum for all engaging with the future of the Internet, to rationalize the discourse and to shatter commonly held assumptions.

Our introduction is followed by five chapters that serve to structure the book: (1) Rights and Rules, (2) Security and Safety, (3) Inclusion and Integration, (4) Infrastructure and Innovation and (5) Data and Disruption.

The book appears in English and contains summaries in Arabic, Chinese, French, German, Russian and Spanish. The texts will also be available online at internetmyths.eu, together with a complete German version at internetmythen.de.

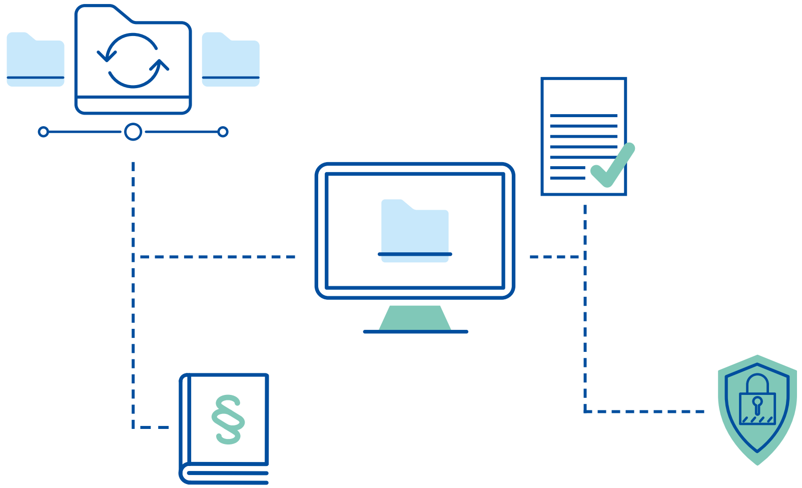
Current and future man, as German philosopher Günther Anders described, meaning people today and people tomorrow, are characterized by a discrepancy between growing technological capacities and the failure of imagination to provide for technology's consequences. Too often myths are used to bridge this gap. But as we show in the course of the 50 myths on the following pages these are just constructs often promulgated by special interests.

Another early German philosopher of technology, Hans Jonas, argued that for technology to work for humans, we need a new "Kompaß", a regulatory polestar, to orient norms and policies. By the early 2000s such a polestar, such a finality, had emerged and would influence the first 15 years of internet governance. In the 2003 Geneva Declaration of Principles and the 2005 Tunis Commitment, the international community confirmed its commitment to build

"a people-centred, inclusive and development-oriented Information Society, premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights, so that people everywhere can create, access, utilize and share information and knowledge, to achieve their full potential and to attain the internationally agreed development goals and objectives, including the Millennium Development Goals."

At this IGF in Berlin, like at the last ones, Internet governance stakeholders discuss how best to achieve this goal. Myths that stand in the way of the commitment need to be busted. This happens to the first 50 myths on the following pages.

Matthias C. Kettemann and Stephan Dreyer
Hamburg/Berlin • September 2019



CHAPTER 1

Rights and Rules

Rechte und Regeln

الحقوق والقواعد

权利和规则

Droits et règles

Права и правила

Derechos y normas

MYTH #01

Nikolas Guggenberger

What people do on the Internet cannot be regulated.

Myth: The Internet cannot be regulated. Human behaviour on the Internet resists all or at least meaningful regulation. Laws either do not apply or, if they apply and are broken, cannot be enforced by the state because of the architecture of the infrastructure and the nature of online communication.

Busted: Despite all evidence to the contrary, the myth that behaviour on the Internet, in cyberspace, or on the "information superhighway" cannot be regulated has prevailed in principle and resurrected in new clothes with every cycle of innovation. The myth builds on both, a misconception of the very nature of regulation and a misunderstanding of the network's infrastructure and the characteristics of online communication in general. Thirty years of scholarship, legislation, and enforcement actions have debunked this myth, and, yet, with every new phenomenon from search engines to social media and Blockchain technology, the myth re-emerges.

Let us start with the misconception of the nature of regulations. Regulations address persons, natural or legal persons to be precise. Regulations do not directly regulate things, including networks, spaces or highways of all sorts, but, at best, relationships between persons and things. Therefore, the question whether the Internet itself can be regulated directly would be the wrong question to ask. Rather, the question to ask is whether persons communicating or transacting via the Internet can be addressed by regulations and whether that in turn shapes the gestalt of the Internet. Phrased correctly, we can clearly answer the question in the affirmative: Persons can be punished for online fraud, they can be held accountable for copyright violations and for distributing illegal content. Electronic contracts are legally binding just as their analogue equivalents. Consumer protection rights have shaped the practice of e-commerce, and the GDPR and its predecessors have defined the boundaries of processing personal data.

The second misunderstanding confuses certain shortcomings in the practical enforcement of legal provisions and the ability to regulate in general.
No doubt, the digital, global, partially decentralized, and in certain ways anonymous environment online promotes certain crimes and eases the circumvention of local rules by lowering transaction costs for such practices (→ #5). However, none of these challenges to law enforcement would undermine the ability to regulate online conduct. First, the competent authorities have developed approaches to investigate crimes and enforce rules online. Second, the Internet as a network and intermediaries depend on physical infrastructure, which can easily be targeted by enforcement actions. Third, the Internet is by no means an environment in which supervision, for systemic reasons, is substantially more difficult than elsewhere.

Truth: Behaviour on the Internet can be subjected to regulation just as any other behaviour. Laws and regulations apply and breaches trigger enforcement actions. Though anonymity, the cross-border character of contracts and crimes, the speed of communication and technical prowess of criminals challenge the effectiveness of law enforcement, this does not change the simple fact that online just as offline, our lives are subjected to regulation.

Source

Lawrence Lessig, Code Version 2.0 (Cambridge: Basic Books).

MYTH #01

Was man im Internet tut, lässt sich nicht regulieren.

Nein, sagt Nikolas Guggenberger: Das Verhalten im Internet kann wie jedes andere Verhalten Gegenstand von Regulierung sein. Gesetze und Vorschriften gelten und Verstöße lösen Rechtsfolgen aus. Auch wenn Anonymität, der grenzüberschreitende Charakter von Verträgen und Straftaten, die Geschwindigkeit der Kommunikation und die technischen Fähigkeiten von Kriminellen Herausforderungen an die Wirksamkeit von Strafverfolgungsmaßnahmen stellen, ändert dies nichts an der einfachen Tatsache, dass unser Leben online ebenso wie offline Regulierung unterworfen ist.

ما يفعله الناس على الإنترنت لا يمكن إخضاعه للتنظيم.

كلا، هكذا يقول نيكولاس غوغنبرغر: يمكن إخضاع السلوك على الإنترنت للتنظيم كأي سلوك آخر، حيث تُطبَّق القوانين واللوائح التنظيمية، أما الانتهاكات فيترتب عليها اتخاذ إجراءات تنفيذية. على الرغم من أن إخفاء الهوية والطابع العابر للحدود الذي يميز العقود والجرائم بالإضافة إلى سرعة الاتصال والبراعة الفنية التي يتمتع بها المجرمون كلها أمور تتحدى فعالية إنفاذ القانون، إلا أن هذا لا يُغيِّر حقيقة بسيطة وهي أن حياتنا بأكملها تخضع للتنظيم، سواء أثناء الاتصال أو دون اتصال.

人们在互联网上所做的事情无法受到监管。

不，Nikolas Guggenberger 写道：像其他行为一样，互联网上的行为也会受到监管。法律和法规都有效，且违法行为会触发执法行动。虽然匿名、合同和犯罪的跨境性质、犯罪分子的通讯速度和技术实力令执法更加困难，但这并未改变我们线上和线下生活均受到监管的简单事实。

Ce que les gens font sur Internet ne peut être réglementé.

Non, écrit Nikolas Guggenberger: les comportements sur Internet peuvent être soumis à une réglementation, comme n‘importe quel autre comportement. Les lois et les règlements s‘appliquent et les infractions entraînent des mesures coercitives. Bien que l’anonymat, le caractère transfrontalier des contrats et des crimes, la rapidité de communication et les prouesses techniques des criminels remettent en question l’efficacité de l’application de la loi, cela ne change rien au simple fait qu’en ligne comme ailleurs, nos vies sont soumises à des règles.

Активность людей в Интернете невозможно регулировать.

Это не так, говорит Николас Гуггенбергер: Как и любую другую, активность в Интернете можно регулировать. Правовые нормы никто не отменял, и их нарушение влечет за собой меры воздействия. Анонимность, международный характер сделок и правонарушений, скорость взаимодействия и техническая подкованность преступников ставят под сомнение эффективность системы охраны правопорядка, впрочем, это не отменяет того простого факта, что наша жизнь регулируется как онлайн, так и офлайн.

No es posible regular lo que las personas hacen en el internet.

No, dice Nikolas Guggenberger: el comportamiento en el internet está sujeto a regulaciones al igual que cualquier otro tipo de conducta. Existen leyes y regulaciones y su incumplimiento conlleva sanciones. A pesar de que el anonimato, el carácter transfronterizo de los contratos y crímenes, la velocidad de la comunicación y la destreza técnica de los criminales dificultan la aplicación efectiva de la ley, esto no altera el simple hecho de que, tanto en el mundo “online” como en el “offline”, nuestras vidas están sujetas a leyes.

MYTH #02

Matthias C. Kettemann

International law does not apply on the Internet.

Myth: Since there is no international treaty regarding the Internet, along the lines of the Paris Agreement on climate change, international law does not apply to international subjects and their relations on, and mediated by, the Internet. States can do what they want online.

Busted: True enough: there is no one international treaty regulating cyberspace. But international law applies to the Internet fully and protects the security, stability, robustness, resilience and functionality of the Internet – its integrity – as a matter of common interest. Already the 2013 report of the UN Group of Governmental Experts, building on the Geneva and Tunis documents, confirmed that applying norms derived from existing international law relevant to the use of ICTs by states "is an essential measure to reduce risks to international peace, security and stability". In its 2015 report, the Group went further and identified the commitment by states to certain key principles of the Charter and other international law as centrally important. These include sovereign equality, prohibition of the threat or use of force, respect for human rights and fundamental freedoms and non-intervention in the internal affairs of other states.

Apart from customary international law, general principles of international law also apply to online settings. These include the principles of due diligence and good neighbourliness which are implemented through confidence-building and capacity-building measures.

There is also a normative argument to be made for applying international law to the Internet: it is "necessary" law. International law is the only body of the law that can serve as the legitimate foundation of an internationally applicable order of norms, through which the exercise of international public authority can be legitimated and the distribution of goods and rights contested and discussed.

The Internet's public core and the servers necessary for it to function are both indispensable for critical infrastructure (e.g. power grids) to work and, in themselves, critical (information) infrastructure. Safeguarding the Internet's integrity (its security, stability, robustness, resilience and functionality) has both become an essential goal for international law and can only be ensured by international law.

International law of the Internet also provides the frame in which Internet governance approaches take place, the "practice" of regulating the Internet (→ #1). Their relevance lies also in the observation that on the Internet the question of legality/illegality is often a false dichotomy. While law traditionally focused on that binarity, governance norms allow for the conceptualization and critique of regimes of responsibility and accountability: there are many shades of legality online. In light of the dynamic nature of the Internet, this variable normativity is a key characteristic of normative evolution.

Truth: While there is no international treaty dedicated to the Internet, international law fully applies. Customary rules and general principles of international law define the power and limits of international actors and, as is common with international law, almost all states respect almost all rules. When more policy-oriented questions need to be solved, Internet governance approaches complement international law.

Source

Group of Governmental Experts Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 of 22 July 2015; Matthias C. Kettemann, The Common Interest in the Protection of the Internet: An International Legal Perspective, in Benedek/de Feyter/Kettemann/Voigt (eds.), The Common Interest in International Law (Antwerp: Intersentia, 2014), 167-184.

MYTH #02

Im Internet gilt kein Völkerrecht.

Nein, sagt Matthias C. Kettemann: Auch ohne einen internationalen Internet-Vertrag gilt das Völkerrecht in vollem Umfang für internetbasierte Informations- und Kommunikationsströme und die diesen zugrunde liegende Infrastruktur. Völkergewohnheitsrechtliche Regeln, darunter das Prinzip der Nichteinmischung, sowie allgemeine Grundsätze des Völkerrechts, wie beispielsweise der Grundsatz der gebotenen Sorgfalt, bilden den normativen Rahmen für das Verhalten internationaler Rechtssubjekte. Internet Governance ergänzt das Völkerrecht.

القانون الدولي لا يسري على الإنترنت.

[كلا، هكذا يقول ماتياس سي كيتيمان: على الرغم من عدم وجود معاهدة دولية مخصصة للإنترنت، إلا أن القانون الدولي يسري تمامًا على تدفقات المعلومات والاتصالات عبر الإنترنت والبنية التحتية التي تدعم هذه المعلومات والاتصالات. وعادةً ما تُشكل النظم العرفية كعدم التدخل، بالإضافة إلى المبادئ العامة للقانون الدولي كمبدأ العناية الواجبة إطاراً معيارياً لموضوعات القانون الدولي. طُرُق إدارة الإنترنت تتمم القانون الدولي.

国际法不适用于互联网。

不，Matthias C. Kettemann 写道：虽然没有专门针对互联网的国际条约，但国际法完全适用于基于互联网的信息和传播流及支持其的基础设施。惯例规则（例如：不干涉原则）和国际法的一般原则（例如：尽职调查原则）规范性地限定了国际法律主体的行为。互联网治理方法是对国际法的补充。

Le droit international ne s‘applique pas sur Internet.

Non, écrit Matthias C. Kettemann: bien qu‘il n‘y ait pas de traité international spécifique à Internet, le droit international s‘applique pleinement aux flux d‘informations et de communication circulant sur Internet et l‘infrastructure attenante. Les règles coutumières, comme la non-intervention, et les principes généraux du droit international, comme le principe de diligence raisonnable ou de vérification préalable, encadrent de façon normative le traitement des sujets liés au droit international. Les approches de la gouvernance d’Internet viennent compléter le droit international.

Международное право не распространяется на Интернет.

Это не так, говорит Матиас К. Каттеманн: Несмотря на отсутствие международного договора, посвященного Интернету, международное право в полной мере применяется по отношению к информационным и коммуникационным интернет-потокам и обслуживающей их инфраструктуре. Нормы обычного права, такие как невмешательство, и общие принципы международного права, как принцип должной осмотрительности, определяют поведение субъектов международного права. Международное право дополняется подходами к управлению Интернетом.

El derecho internacional no se aplica al internet.

No, dice Matthias C. Kettemann: si bien no existe un tratado internacional dedicado al internet, el derecho internacional se aplica plenamente a la información del internet, a los flujos de comunicación y a la infraestructura que les subyace. Las normas consuetudinarias, como la de no intervención, así como otros principios generales del derecho internacional como el principio de diligencia debida, ponen marcos normativos al comportamiento de los sujetos internacionales de derecho. Los enfoques de gobernanza del internet complementan al derecho internacional.

MYTH #03

Riikka Kuolu

Code is law.

Myth: Code is law. The software codes have become focal, or even the primary tool for regulating human behaviour and asserting social control. The Internet is also averse to governmental regulation and thus in need of alternative strategies such as self-regulation and regulation by code.

Busted: It is undeniable that coded environments have a normative dimension that influences possible actions of Internet users. However, this does not mean that existing societal and legal structures would automatically disappear or become inefficient in online environments; and neither was this Lessig's original argument. According to Lessig, technical infrastructure is only one form of cyberspace regulations alongside with law, social norms, and the market. Lessig's stance can be seen to represent cyberpaternalism, as it depicts concern for the covert, opaque and insidious control that the codes presents, which in Lessig's view needs to be remedied by legislations and transparency of both online and offline regulations.

Ultimately, code is law is an oversimplification of a much more complex regulatory landscape, reflecting the disbelief in the states' ability to regulate cyberspace as coined in the 1996 Declaration of Independence Cyberspace and often misquoted for political ends. (→ #1) The approach does not take into account that modern law is not bound to the state but is also international and pluralistic. (→#2) Hence, transnational nature of Internet does not mean that online behaviour would remain beyond the grasp of state and non-state offline actors, as e.g. the attempts to regulate platforms, data governance, and consumer protection in e-commerce demonstrate.

Lessig's observation that in cyberspace social control is exerted through technological architecture holds true. It also reflects earlier insights into normative technologies, which focused on social engineering through architecture and technological artefacts. As Leenes describes, code is law resembles other "design-based control mechanisms [that] are extremely powerful because they act ex ante rather than ex post" and that do not involve sanctions in the typical sense (Leenes 2012, 147). Technical infrastructure is not sufficient, as it is not able to entirely remove conflicts, which then require ex post mechanisms for dispute resolutions provided by law.

The normativity of technology differs from legal normativity. Hildebrandt describes technological normativity as "the way a particular technological device or infrastructure actually constrains human actions, inviting or enforcing, inhibiting or prohibiting types of behavior". Unlike legal normativity, technological architecture does not rely on the state's authority and monopoly of violence nor is it produced through democratic procedure (Hildebrandt 2008, 176).

Truth: Socio-legal scholarship has produced a more complex and nuanced approach to describe the intricate interplay of technical, legal, and social rules that define and regulate human behaviour online. For example, concepts of legal pluralism or techno-regulation can be used to describe the complexity of Internet regulation that consists of multiple state and non-state actors and layers of legal, social, and technical regulation.

Source

Mireille Hildebrandt, Legal and Technological Normativity: More (and Less) Than Twin Sisters (2008) 12(3) Techné: Journal of the Society for Philosophy and Technology (2008), 169-183, https://www.academia.edu/702733/Legal_and_Technological_Normativity_more_and_less_than_twin_sisters; Ronald Leenes: Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology, Tilburg Law School Legal Studies Research Paper Series No. 10/2012, available at: http://ssrn.com/abstract=2182439.

MYTH
#03

Code ist Gesetz.

Nein, sagt Riikka Kuolu: Die rechtssoziologische Forschung hat einen komplexeren und differenzierteren Ansatz zur Beschreibung des komplizierten Zusammenspiels technischer, rechtlicher und gesellschaftlicher Regeln für die Regelung menschlichen Verhaltens im Netz formuliert. So können beispielsweise Konzepte des rechtlichen Pluralismus oder der Technoregulierung zur Beschreibung der Komplexität der Internetregulierung hilfreich sein, um die Vielzahl staatlicher und nichtstaatlicher Akteure sowie die verschiedenen Schichten rechtlicher, gesellschaftlicher und technischer Regulierung passend zu fassen.

الكود هو القانون.

كلا، هكذا تقول ريكا كولو: تمخضت المعرفة الاجتماعية القانونية عن طُرُق أكثر دقة وتعقيدًا لوصف التفاعل المعقد بين القواعد الفنية والقانونية والاجتماعية التي تحدد وتنظم السلوك البشري أثناء الاتصال. فعلى سبيل المثال، يمكن استخدام مفاهيم التعددية القانونية أو التنظيم الفني لوصف تعقيد تنظيم الإنترنت الذي يتألف من العديد من الجهات الفاعلة الرسمية وغير الرسمية وطبقات متعددة من اللوائح التنظيمية القانونية والاجتماعية والفنية.

代码即法律。

不，Kuolu 写道：社会-法律学术研究产生了一种更为复杂和细致入微的方法，用于描述定义和规范网络行为的技术、法律和社会规则之间的复杂相互作用。例如，法律多元化或技术监管的概念可用于描述由多个国家和非国家行为者以及法律、社会和技术监管层组成的互联网监管的复杂性。

Le code, c‘est la loi.

Non, écrit Riikka Kuolu: les recherches sociojuridiques ont apporté une approche plus complexe et nuancée pour décrire l’interaction complexe de règles techniques, juridiques et sociales qui définissent et réglementent le comportement humain en ligne. Par exemple, les concepts de pluralisme juridique ou de techno-régulation peuvent être utilisés pour décrire la complexité de la régulation d’Internet composée de multiples acteurs gouvernementaux et non-gouvernementaux et de multiples couches de régulations juridiques, sociales et techniques.

Код – это закон.

Это не так, говорит Рийкка Кулу: Социо-правовые науки выработали более сложный и гибкий подход к отображению замысловатого взаимодействия между техническими, юридическими и социальными правилами, которые определяют и регулируют онлайн-активность. К примеру, с помощью концепции правового плюрализма или технического регулирования можно объяснить комплексность регулирования Интернета, что включает в себя множество государственных и негосударственных участников, а также уровней юридического, социального и технического регулирования.

La ley la dicta el código.

No, dice Riikka Kuolu: los estudios socio-jurídicos han producido un enfoque más complejo y matizado para describir la compleja interrelación de normas técnicas, legales y sociales que definen y regulan el comportamiento humano en el internet. Pueden usarse, por ejemplo, conceptos de pluralismo jurídico y de normativa técnica para describir la complejidad de la regulación del internet, la cual consta de múltiples actores estatales y no-estatales, así como de estratos de reglamentación legal, social y técnica.

MYTH
#04

Corinne Cath-Speth

Protocols do not have politics.

Myth: The technical standards and protocols upon which the Internet is built do not have politics. Rather, they are neutral technologies developed by impartial engineers, through apolitical consensus mechanisms, who merely want information to flow and networks to internetwork.

Busted: It can be hard to see the politics of protocols through the fog of enigmatic Internet standardization acronyms. Protocol developers' penchant for dense abbreviations of abbreviations, like Domain Name System (DNS) over Transport Layer Secure (TLS) or DoT, does not help in that regard. Some background: The Internet runs on a set of technical standards and protocols. The first iteration of the Internet came out of the need for disparate networks to talk to each other. (→ #15) Internet protocols enabled such "internetworking" to occur by providing a standardized manner for networks to exchange information. These protocols are developed by industry-led standard-setting bodies, like the Internet Engineering Task Force (IETF). Many within these organizations hold that protocols do not have politics; protocols are seen as neutral, it's in how people use them that they have moral and political impact.

This is a myth because it presumes that these technical organizations are somehow detached from their larger context and that protocols are neutral tools. But protocols are built by people, who encode their values, ideologies and assumptions. (→#18; → #42) Protocols do have politics. The question is: whose? Take DoT as an example: its designers prioritized user privacy over commercial or government access to data about what website users visit. This prioritization, in turn, influences how power struggles between different stakeholders (governments, industry, civil society) over online information flows materialize.

The inherent "politics of protocols" is hardly surprising to those experiencing or studying its effects. In his landmark 1980's essay, Langdon Winner showed that technology is not value neutral, as it reflects distinct moral and political choices. More recently, Laura DeNardis argued that protocols have politics because they mediate social and political values through technology, which in turn shape society. Likewise, communities affected by protocol design – whether representing specific disability justice concerns around website accessibility or broad human rights concerns like privacy – have highlighted the inherent politics of protocols. Yet, among many in the technical community the myth that protocols do not have politics persists, sometimes to the detriment of Internet users.

Truth: Upholding that 'protocols do not have politics' is inherently a form of politics, because it implies a commitment to the status quo – which often aligns with Global North values and industry interests – driving Internet standardization. It also overlooks how Internet standardization occurs within distinct cultural, economic and political conditions. Protocols have politics and further critical engagement with the consequences of these politics is needed.

Source

Laura DeNardis, Protocol Politics: The Globalization of Internet Governance (Boston: MIT Press, 2013); Corinne Cath and Luciano Floridi, The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights, Science and Engineering Ethics 23 (2017) 2, 449-468.

MYTH #04

Protokolle sind unpolitisch.

Nein, sagt Corinne Cath-Speth: Die Behauptung, dass Protokolle unpolitisch seien, ist bereits eine Form von Politik, impliziert sie doch ein Bekenntnis zum – oftmals den Werten und Interessen der Industriestaaten und Wirtschaftsakteure entsprechenden – Status quo und begünstigt die weitere Standardisierung des Internets. Auch wird hierbei übersehen, wie die Standardisierung des Internets im Kontext unterschiedlicher kultureller, wirtschaftlicher und politischer Bedingungen erfolgt. Protokolle sind politisch und es bedarf einer weiteren kritischen Auseinandersetzung mit den Folgen dieser Politik.

البروتوكولات لا تنطوي على سياسة.

كلا، هكذا تقول كورين كاث-سبيث: تأكيدنا أن «البروتوكولات لا تنطوي على سياسة» في حد ذاته شكل من أشكال السياسة؛ لأنه ينطوي على التزام بالوضع الراهن الناظم لمسيرة التوحيد القياسي للإنترنت والذي يتطابق ضمناً في كثير من الأحيان مع قيم بلدان الشمال ومصالح القطاع الصناعي. كما أنه يتجاهل أيضًا كيف يحدث التوحيد القياسي للإنترنت في ظل ظروف ثقافية واقتصادية وسياسية متباينة. فالبروتوكولات تنطوي على سياسة، وهناك حاجة إلى المزيد من الانخراط حاسم الأهمية مع عواقب هذه السياسة.

网络协议不涉及政治。

不，Corinne Cath-Speth 写道：赞成“网络协议不涉及政治”本质上是一种政治形式，因为它意味着对现状的承诺，通常与北半球的价值观和行业利益一致，即推动互联网标准化。它还忽略了互联网标准化在不同的文化、经济和政治条件下发生的方式。网络协议涉及政治，且需要进一步批判性地参与政治成果。

Les protocoles ne font pas de politique.

Non, écrit Corinne Cath-Speth: soutenir le fait que « les protocoles ne font pas de politique » est intrinsèquement une forme de politique, car cela implique un engagement envers le statu quo, souvent aligné sur les valeurs du Nord et les intérêts de l'industrie, et qui serait à la base de la normalisation d'Internet. Cela néglige également la manière dont la normalisation d'Internet se produit dans des environnements culturels, économiques et politiques différents. Les protocoles font de la politique et un engagement critique supplémentaire vis-à-vis des conséquences de cette politique est nécessaire.

Политика не применима к протоколам.

Это не так, говорит Корин Кэт-Спет: Утверждение о том, что политика не применима к протоколам уже само по себе форма политики, ведь оно косвенно выражает приверженность идее «статуса-кво», а это в свою очередь зачастую соответствует ценностям и экономическим интересам так называемых «стран Севера», стимулируя онлайн-стандартизацию. Также оно игнорирует то, как происходит онлайн-стандартизация в условиях разных культурных, экономических и политических факторов. Политика применима к протоколам и дальнейшая критичная реакция на последствия такой политики просто необходима.

Los protocolos están exentos de política.

No, dice Corinne Cath-Speth: el hecho de sostener que “los protocolos están exentos de política” es ya en sí mismo una forma de política, puesto que implica un compromiso con el orden establecido (el cual frecuentemente se alinea a los valores e intereses industriales del Norte Global) que promueve la estandarización del internet. También pasa por alto la manera en la que esta estandarización del internet ocurre en medio de condiciones culturales, económicas y políticas distintas. Los protocolos implican política y se requiere un compromiso crítico mayor con las consecuencias de dicha política.

MYTH #05

Amadeus Peters

Cybercriminals go free.

Myth: Anonymity on the Internet is highly valued by criminals. To hide their identity they use anonymizers like the Tor browser, which also allows access to the darknet, and they ask to be paid in cryptocurrencies like Bitcoin. This makes it impossible for the police to catch cybercriminals.

Busted: Even though there are many good tools to disguise one‘s identity, law enforcement agencies worldwide have caught many cybercriminals with low and high profiles. This also applies to customers, traders and platform administrators of darknet markets (→ #17), where drugs, counterfeit money, and weapons are traded like on Amazon.

A particularly good example is the multinational police operation “Bayonet” in 2017. The Dutch police received a tip from a company that had stumbled upon a server that was used to test a new feature for the darknet website Hansa. Hansa was the world‘s third-largest darknet market at the time. The Dutch police monitored the connections established with the server and was thereby able to identify the server hosting the actual Hansa website. They secretly made a copy of the stored data and found very old chat logs with the real names of administrators.

For unknown reasons, the website was quickly moved to new unknown servers. The new hosting provider who had been identified in the data collected on the previous server was paid with Bitcoins. Since the transactions in the Bitcoin blockchain are public, the payments could be tracked until the bitcoins were exchanged into euros. The Bitcoin exchange then disclosed their customer, the new hosting provider, upon request.

The German police arrested the administrators, while the Dutch police secretly took control of the Hansa website and police officers pretended to be the administrators. The Dutch police made changes to the encrypted communications between customers and dealers, providing them with 10,000 delivery addresses. Simulating technical issues, they had all dealers re-upload product images to get the geolocations stored in the metadata, which put them on the trail of 50 sellers. In addition, they tricked 64 sellers into opening a file that would reveal their real IP address. After having collected all that data, the website was closed down and the police started prosecuting customers and dealers.

This example shows how law enforcement agencies can not only overcome anonymity but also benefit from it. Furthermore, to receive goods or money paid out in a conventional currency one has to leave the virtual world and thus relinquish anonymity at some point.

Truth: Cybercriminals get caught despite anonymization tools because human error and random events - which can provide the crucial clues to overcome anonymity - cannot be ruled out. Additionally, many popular cryptocurrencies do not anonymize transactions, but only pseudonymize them, allowing money flows to be analyzed and tracked. This allows police services to make arrests in the real world.

Source

Y. Danny Huang et al., Tracking Ransomware End-to-end, IEEE Symposium on Security and Privacy (2018), https://ieeexplore.ieee.org/document/8418627; Jonathan Lusthaus, Industry of Anonymity (Cambridge, MA: Harvard University Press, 2018).

MYTH #05

Cyberkriminelle brauchen keine Strafe zu fürchten.

Nein, sagt Amadeus Peters: Cyberkriminelle werden trotz Anonymisierungstools erwischt, da menschliches Versagen und Zufall – wodurch sich entscheidende Hinweise zur Überwindung der Anonymität ergeben können – nicht ausgeschlossen werden können. Darüber hinaus werden bei vielen gängigen Kryptowährungen Transaktionen nicht anonymisiert, sondern lediglich pseudonymisiert, sodass Zahlungsströme analysiert werden können und die Polizei dann in der realen Welt zur Verhaftung schreiten kann.

المجرمون السيبرانيون ينجون من العقوبة.

كلا، هكذا يقول أماديوس بيترز: يتم القبض على المجرمين السيبرانيين على الرغم من أدوات إخفاء الهوية؛ لأنه لا يمكن استبعاد الخطأ البشري والأحداث العشوائية التي يمكنها تقديم خيوط بالغة الأهمية للتغلب على خفاء الهوية. بالإضافة إلى ذلك فإن كثيرًا من العملات المشفرة لا تخفي هوية المعاملات بل تعطيها اسمًا مستعارًا فحسب مما يسمح بتحليل حركات التداولات المالية، مما يسمح لأجهزة الشرطة بتنفيذ اعتقالات في العالم الحقيقي.

网络犯罪分子可以逍遥法外。

不，Amadeus Peters 写道：尽管有匿名化工具，网络犯罪分子仍会被抓获，因为无法排除的人为错误和随机事件可提供克服匿名的关键线索。此外，许多流行的加密货币不会对交易进行匿名化，而仅对交易进行假名化，因而可以分析资金流向。这使得警方能在现实世界中完成抓捕。

Les cybercriminels ne sont pas arrêtés.

Non, écrit Amadeus Peters: les cybercriminels se font prendre malgré les outils d'anonymisation, car les erreurs humaines et les événements aléatoires, qui peuvent fournir des indices essentiels pour venir à bout de l'anonymat, ne peuvent être exclus. En outre, de nombreuses cryptodevises populaires ne rendent pas les transactions anonymes, elles les pseudonymisent, ce qui permet d'analyser les flux monétaires. Cette analyse permet de surcroît à la police de procéder à des arrestations dans le monde réel.

Киберпреступникам все сходит с рук.

Это не так, говорит Амадей Петерс: Несмотря на все доступные инструменты анонимизации, киберпреступники все же попадаются, ведь человеческий фактор и случайные события невозможно исключить, и именно они могут стать ключом к победе над анонимностью. К тому же, большинство популярных криптовалют не анонимизируют операции, а только псевдонимизируют их, что дает возможность анализировать денежные потоки. Это позволяет правоохранительным органам производить аресты в реальном мире.

Los ciberdelincuentes viven en libertad.

No, dice Amadeus Peters: los ciberdelincuentes son atrapados a pesar de usar herramientas de anonimización, ya que los factores de error humano y los eventos fortuitos, los cuales pueden proporcionar las pistas clave para desvelar su anonimato, nunca pueden descartarse. Además, muchas criptomonedas populares no anonimizan sus transacciones, sino que solamente las seudonimizan, lo cual hace posible analizar los flujos de dinero. Esto a su vez permite a la policía hacer arrestos en el mundo real.

MYTH #06

Emily Laidlaw

You can say what you want online.

Myth: The Internet is a free-for-all space where hate speech, defamation and other forms of abuse can be expressed without limits or consequences. If a person posts something abusive on a social networking site, for example, this is protected expression, and there are no avenues through the law or otherwise to restrain that behaviour.

Busted: Many things limit what you say online, including laws, norms, community standards, advocacy, artificial intelligence and the market. All of these different modalities of regulations form the system of governance of online expression. (→ #1, → #2) In this system, human rights are the central conceptual reference point (even if there is significant debate about how to balance human rights in difficult cases). Human rights law protects the right to freedom of expression as integral to a thriving democracy, to our sense of dignity and autonomy and search for the truth. However, the right comes with responsibilities, such as to not infringe upon the rights of others to their reputation or privacy, for national security or protection of public health or morals.

This idea of speech as a right and responsibility infiltrates all the different layers in the system of governance online. Domestic constitutions tend to frame freedom of expression this way. Criminal and civil laws prohibit certain forms of speech that are seen as particularly harmful to society, such as incitement to hatred, promotion of genocide, defamation or terrorist speech. A particular challenge online is that the offenders are often difficult to track down (→ #5), whether because they are located out of jurisdiction or post anonymously (although often identifiable) and speech is routed through a private intermediary. Thus, traditional command and control laws can be less effective in restraining illegal speech.

However, other forms of regulations help fill that gap, at times innovative and at other times crude. The terms and conditions of use on social networking platforms create their own limits on the right to freedom of expression, such as nudity or extreme violence. Artificial intelligence is increasingly used to ensure compliance by identifying and removing content. On some sites, the community of users regulates speech through informal social norms, such as rules of moderators, although this can spur other forms of harmful speech through mobs. Civil society and communities regulate speech by advocating for platforms to remove or put back certain content or groups. And the market regulates speech by providing alternatives to users or is hampered as a regulator through tech dominance and power.

Truth: The Internet is not a free speech paradise where anything can be posted without consequence. Rather, online speech is regulated through a complex system of governance, including laws, norms, community standards, advocacy, artificial intelligence and the market. The question is not whether you can say anything you want online – you can't – but rather how to design the system managing free expression to be more effective and sensitive to human rights principles.

Source
Emily Laidlaw, Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility (Cambridge University Press, 2015); David Kaye, Speech Police: the Global Struggle to Govern the Internet (Columbia Global Reports, 2019).

MYTH #06

Online kann man sagen, was man will.

Nein, sagt Emily Laidlaw: Das Internet ist kein Paradies freier Meinungsäußerung, in dem alles ohne Konsequenzen veröffentlicht werden kann. Vielmehr werden Onlineäußerungen durch ein komplexes Governance-System aus Gesetzen, Normen, gesellschaftlichen Standards, Interessenverbänden, künstlicher Intelligenz und dem Markt geregelt. Die Frage ist nicht, ob man online sagen kann, was man will – was nicht der Fall ist –, sondern vielmehr, wie man das System der freien Meinungsäußerung so gestalten kann, dass es effektiver und menschenrechtssensibler angewandt wird.

يمكنك قول ما تريد على الإنترنت.

كلا، هكذا تقول إميلي لايدلو: ليست الإنترنت فردوسًا لحرية التعبير حيث ننشر ما نشاء دون تحمل أي عواقب. بل على العكس، حيث يتم تنظيم الحوار الالكتروني من خلال نظام إدارة معقد يشتمل على القوانين والأعراف والمعايير المجتمعية والمناصرة والذكاء الاصطناعي والسوق. وليست المسألة ما إن كنت تستطيع قول ما تشاء على الإنترنت أم لا - فأنت لا تستطيع ذلك - بل بالأحرى كيفية تصميم النظام الذي يدير حرية التعبير ليكون أكثر فعالية وحساسية تجاه مبادئ حقوق الإنسان.

在网上想说什么就能说什么。

不，Emily Laidlaw 写道：互联网并非言论自由的天堂，发布内容之前也必须考虑后果。更确切地说，网络上的言论是通过复杂的治理体系进行规管的，包括法律、规范、社区标准、倡导、人工智能和市场。问题不在于您是否可以想说什么就说什么（不行！），而是如何设计管理自由表达的系统，使其更加有效和更容易受到人权原则的影响。

En ligne, on peut dire ce que l‘on veut.

Non, écrit Emily Laidlaw: Internet n‘est pas le paradis de la liberté d‘expression où tout peut être publié sans conséquence. Au contraire, la parole en ligne est régie par un système complexe de gouvernance, comprenant des lois, des normes, des standards collectifs, la défense des droits, l‘intelligence artificielle et le marché. La question n‘est pas de savoir si vous pouvez dire ce que vous voulez en ligne puisque ce n’est pas le cas, mais plutôt de savoir comment concevoir le système de gestion de la liberté d‘expression pour qu‘il soit plus efficace et plus sensible aux principes des droits de l‘Homme.

В Интернете можно говорить все, что пожелаешь.

Это не так, говорит Эмили Лэйдлоу: Интернет – это не рай свободы слова, где вы можете публиковать что угодно без каких-либо последствий. На самом деле высказывания в Интернете регулируются сложной системой управления, которая включает в себя законы, нормы, общественные стандарты, защиту интересов, искусственный интеллект и рынок. Дело не в том, можете ли вы говорить все, что захотите онлайн – не можете – а скорее в том, как сделать систему свободы слова более эффективной и чувствительной к принципам прав человека.

En el internet puedes decir cualquier cosa que desees.

No, dice Emily Laidlaw: el internet no es un paraíso de libre expresión, en donde cualquier cosa puede ser posteada sin consecuencias. Más bien, el discurso online está regulado por un complejo sistema de gobernanza, el cual incluye leyes, normas, estándares comunitarios, defensa, inteligencia artificial y al mercado. La pregunta no sería si puedes o no decir lo que quieras en el internet (no puedes), sino cómo hay que diseñar el sistema regulador de la libre expresión para que sea más efectivo y tenga en cuenta los principios de los derechos humanos.

MYTH #07

Amélie Pia Heldt

Internet platforms are not liable for user-generated content.

Myth: Internet platforms are merely a conduit for user-generated content. They function like a pipe and do not look at the content itself, which is why they are neither liable nor responsible for unlawful content uploaded by their users.

Busted: Originally, Internet platforms were thought of as distributors, not publishers: content-neutral platforms that enable their users to share content without verifying or curating it. This principle was translated into a landmark U.S. Internet legislation, section 230 of the 1996 Communications Decency Act (hereinafter Sec. 230 CDA), according to which (simply put) no “interactive computer service” should be treated as a publisher or a speaker, hence should not be liable for what had been expressed by means of user-generated content (UGC). Internet platforms would only be liable for UGC in cases of federal criminal liability and intellectual property claims, or when performing an editorial role. The origin of this law can be found in a decision by the Supreme Court (Smith v. California) concerning the liability of a book store owner compared to an author’s or publisher’s liability: the Court held that one could not be held criminally liable without knowledge of content, that is, for just possessing a book containing obscene images. Such regulation of liability was deemed unconstitutional under the First Amendment although obscene speech itself is not protected.

Other countries have adopted similar legislation, e.g. section 79 of the Indian Information Technology Act, which provides a qualified immunity for intermediaries, or article 14 of the EU’s E-Commerce Directive 2000/31/EC.

However, there has been a noticeable change over the past five years: the EU judiciary and the European legislator have moved towards a tighter liability for platforms. In the course of introducing more balanced responsibility-sharing, the intermediary immunity has been increasingly restricted when it comes to hate speech, terror propaganda, or copyright infringements, e.g. by art. 17 (3) of the 2019 EU Copyright Directive in the Digital Single Market, under which online content-sharing service providers are now liable for copyright infringements. Under the German Network Enforcement Act (2017) platforms have to ensure an efficient complaint procedure for “manifestly unlawful content”. Under certain EU proposals it could also become mandatory for platforms to de facto proactively filter UGC in order to prevent illegal content from being uploaded, but this proposal is highly controversial. (→ #6) All in all, the question of platforms’ liability highlights the differences in speech regulation between the US and the EU.

Apart from the limits imposed by the lawmakers it is the principle itself that has been under attack. The basis of this relative intermediary immunity, that is, their neutrality vis-à-vis the content itself, is in most cases a chimera. Platforms classify, prioritize and moderate UGC. Technology enables them to increasingly identify and remove content before it is flagged by a user, making the analogy of an uninformed book store owner obsolete.

Truth: Internet platforms are not merely neutral distributors of content they neither know nor care about. While the liability of platforms in the US is closely curtailed, European law recognizes a more nuanced responsibility regime, especially with regard to the protection of intellectual property, clearly illegal content and serious offences, such as the promotion of terrorism.

Source

Daphne Keller, Toward a Clearer Conversation About Platform Liability, Knight First Amendment Institute’s “Emerging Threats” Essay Series (2018), https://knightcolumbia.org/content/toward-clearer-conversation-about-platform-liability; Aleksandra Kuczerawy, Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative (2014), Computer Law and Security Review 31 (2015) 1, 46-56; CiTiP Working Paper 21/2015,https://ssrn.com/abstract=2560257.

MYTH
#07

Internetplattformen haften nicht für nutzer*innengenerierte Inhalte.

Nein, sagt Amélie P. Heldt: Internetplattformen sind nicht bloße neutrale Verteiler von Inhalten, die sie weder kennen noch interessieren. Während die Haftung von Plattformen in den USA stark eingeschränkt ist, kennt das europäische Recht differenziertere Verantwortungsregelungen insbesondere in Bezug auf den Schutz geistigen Eigentums, eindeutig rechtswidrige Inhalte und schwere Straftaten wie beispielsweise die Förderung des Terrorismus.

منصات الإنترنت غير مسؤولة عن المحتوى الذي يُنشئه المستخدم.

كلا، هكذا تقول أميلي بي هيلت: منصات الإنترنت ليست مجرد موزعين محايدين لمحتوى لا يعرفونه ولا يبالون به. وعلى الرغم من المحدودية الشديدة لمسؤولية المنصات في الولايات المتحدة، يعترف القانون الأوروبي بنظام مسؤولية أكثر تعقيدًا، ولا سيما فيما يتعلق بحماية الملكية الفكرية والمحتوى المخالف للقانون بشكل واضح بالإضافة إلى الجرائم الخطيرة كالترويج للإرهاب.

互联网平台不对用户生成的内容负责。

不，Amélie P. Heldt 写道：互联网平台不仅仅是既不知晓也不关注内容的中立分销商。虽然美国互联网平台的责任大幅减少，但欧洲法律承认更加细致入微的责任制度，尤其是与知识产权保护、明确的非法内容和严重的违法行为（例如助长恐怖主义）有关的责任制度。

Les plateformes Internet ne sont pas responsables du contenu généré par les utilisateurs.

Non, écrit Amélie P. Heldt: les plateformes Internet ne sont pas de simples distributeurs neutres de contenus dont elles n‘ont pas connaissance et dont elles ne se soucient pas. Alors que la responsabilité des plateformes aux États-Unis est très faible, le droit européen reconnaît un régime de responsabilité plus nuancé, notamment en ce qui concerne la protection de la propriété intellectuelle, les contenus clairement illégaux et les infractions graves, telles que la promotion du terrorisme.

Интернет-платформы не несут ответственности за пользовательский контент.

Это не так, говорит Амели П. Хельдт: Интернет-платформы – это не просто безучастные распространители контента, который их не заботит, и о котором они ничего не знают. Тогда как ответственность платформ достаточно ограничена в США, в Европейском законодательстве закреплен более дифференцированный режим ответственности, в особенности в отношении защиты интеллектуальной собственности, явно незаконного контента и серьезных преступлений, таких как пропаганда терроризма.

Las plataformas del internet no son responsables del contenido generado por los usuarios.

No, dice Amélie P. Heldt: las plataformas del internet no son meramente distribuidores neutrales de contenido que no conocen ni les interesa. Mientras que la responsabilidad de las plataformas en los Estados Unidos está estrechamente acotada, la Ley europea contempla un régimen de responsabilidad más matizado, especialmente en lo que respecta a la protección de la propiedad intelectual, al contenido claramente ilegal y a ofensas serias como la promoción del terrorismo.

MYTH #08

Roxana Radu

The Internet has always run on multistakeholder approaches.

Myth: The decentralized nature of the Internet requires the involvement of various stakeholder groups, such as governments, the industry and civil society. Unlike other policy fields in which intergovernmental approaches dominate, the Internet has, from the outset, been synonymous with multistakeholder governance, offering a seat at the table to all those interested.

Busted: Many accounts of Internet governance uphold its multistakeholder nature as an early achievement, allowing governments, businesses, technical community, academia and civil society to participate in decision-making, whether in consultative roles or as part of collaborative rule-creation efforts. However, the decisions that led to the funding, creation and privatization of the Internet were not the result of multistakeholder processes: they were unilaterally put forward by the US government. Currently ruled by more than 300 authoritative instruments at the global and regional level (and many more at the national level), the Internet is governed through various mechanisms, many of which are exclusively government- or industry-driven.

Frequently contrasted with the intergovernmental model traditionally applied to regulating telecommunications, the multistakeholder approach is widely perceived as the best way to govern the Internet, reflecting certain dynamics set in place by the technical community in the early days of the network. In practice, multistakeholderism is best understood, since its emergence in the mid-1990s, as an anchoring practice of the community. The involvement of representatives belonging to various sectors was prominently practiced during the negotiations around the management of the domain name system (DNS), previously ran singlehandedly by an academic at Stanford University (Jon Postel). In 1998, based on the top-down guidance of the US Department of Commerce implemented via multistakeholder discussions, a new non-for-profit organization was established to perform that function: ICANN. Subsequently, many other organizations started adopting multistakeholder practices and celebrating the broad range of interests they catered for.

Over time, multistakeholderism acquired a strong normative grounding, claiming a distinctive character. Its cross-sector integration in certain activities of intergovernmental bodies, as well as in the work of standard-setting bodies, is a case in point. Its many different forms and shapes (Raymond and DeNardis 2015) have evolved and been institutionalized to a large degree. Beyond the rhetoric, the multistakeholder Internet governance remains ideologically-laden and hides significant power inequalities among stakeholder groups. The promise of participation on an equal footing contrasts sharply with the practice of engagement that privileges the interests of a few and serves to legitimize the decisions of instrumental actors. Institutionally, an approach based on ‘respective roles and responsibilities’ was formally sanctioned in the outcome document of the UN Summit on Information Society held in 2005 and reiterated during its decennial review (WSIS+10). Other global meetings, such as the annual Internet Governance Forum or the 2014 NETMundial, have since proposed procedural improvements.

Truth: Multistakeholderism is a dominant practice adopted by the Internet governance community in the 1990s. Despite its wide appeal, the main Internet policy decisions and the global, regional and national rules that guide its evolution are rarely the result of multistakeholder processes that live up to the rhetoric of engaging government, industry and civil society on an equal footing.

Source

Roxana Radu, Negotiating Internet Governance (Oxford: Oxford University Press, 2019); Mark Raymond and Laura DeNardis, Multistakeholderism: Anatomy of an Inchoate Global Institution, International Theory 7 (2015) 3, 572– 616.

MYTH #08

Policy-Entwicklung im Internet beruht schon immer auf dem Multi-Stakeholder-Ansatz.

Nein, sagt Roxana Radu: Das Multi-Stakeholder-Prinzip ist die seit den 1990er Jahren von der Internet Governance-Community angewandte vorherrschende Praxis. Trotz der großen Attraktivität des Multi-Stakeholder-Prinzips sind die wichtigsten internetpolitischen Entscheidungen und die die Entwicklung des Internets prägenden globalen, regionalen und nationalen Regeln nur selten das Ergebnis von Multi-Stakeholder-Prozessen, die Regierungen, die Industrie und die Zivilgesellschaft gleichberechtigt in ihrer jeweiligen Rolle einbeziehen.

الإنترنت تسير دائمًا وفق نُهج تعدد أصحاب المصالح.

كلا، هكذا تقول روكسانا رادو: يُعد نهج تعدد أصحاب المصالح ممارسة سائدة اعتمدها مجتمع إدارة الإنترنت في التسعينيات. وعلى الرغم من جاذبيته الواسعة إلا أن القرارات الرئيسية المتعلقة بسياسات الإنترنت والقواعد العالمية والإقليمية والوطنية التي توجّه تطورها نادرًا ما تكون نتاج عمليات متعددة لأصحاب المصالح ترقى إلى مستوى خطاب إشراك الحكومة والصناعة والمجتمع المدني على قدم المساواة.

互联网一直以多利益相关方的模式运转。

不，Roxana Radu 写道：多利益主体主义是互联网治理社区在 20 世纪 90 年代采用的一种主导惯例。尽管具有广泛的吸引力，但主要的互联网政策决定以及指导多利益主体主义发展的全球、区域和国家规则，很少是符合平等参与主体政府、行业和民间社会言论的多利益相关方流程的结果。

Internet a toujours fonctionné selon une approche multipartite.

Non, écrit Roxana Radu : le multipartisme est une pratique dominante adoptée par la communauté de gouvernance d‘Internet dans les années 90. Malgré son fort attrait, les principales décisions de politique Internet et les règles mondiales, régionales et nationales qui guident son évolution sont rarement le résultat de processus multipartites respectant la rhétorique consistant à impliquer à part égale les gouvernements, l‘industrie et la société civile.

Интернет всегда функционировал по принципам заинтересованных сторон.

Это не так, говорит Роксана Раду: Участие множества заинтересованных сторон – принятая в 1990-х сообществом управления Интернетом практика. Несмотря на свою огромную привлекательность, основные политические решения в отношении Интернета и глобальные, региональные и национальные правила, определяющие его эволюцию, редко являются результатом процессов с участием множества заинтересованных сторон, которые оправдывают риторику привлечения правительства, промышленности и гражданского общества на равных условиях.

El internet siempre ha funcionado a base de enfoques multilaterales.

No, dice Roxana Radu: el multilateralismo es una práctica dominante adoptada por la comunidad de gobernanza del internet en los años 1990. A pesar de su gran atractivo, las principales decisiones sobre la regulación del internet y las normas globales, regionales y nacionales que han guiado su evolución, raramente han sido resultado de procesos multilaterales a la altura de la retórica de comprometer a los gobiernos, industrias y sociedad civil a un mismo nivel.

MYTH #09

Kurt M. Saunders

On the Internet, everything is free.

Myth: If something is on the Internet, it must be free and in the public domain. Many users hold a false presumption that online media and content is not copyright protected. For others, the belief is subconscious, leading them to copy, share, or adapt content without first considering that they may need authorization by the copyright owner to do so.

Busted: There appear to be two bases for the belief that content found in the Internet is free, or not protected by copyright law, both of which are interrelated. The first basis is technological. The Internet greatly reduces the effective cost of copying, making it easy and inexpensive to access, reproduce, transfer, and manipulate content. Users can reproduce and transfer numerous copies to numerous recipients worldwide instantaneously. The second basis is philosophical and is tersely expressed by the declaration: "Information wants to be free." (→ #48) The statement is attributed to Stewart Brand at the first Hackers Conference in 1984 and it became a rallying cry of the cyberpunk movement (Whole Earth Review (1985), 49). In short, it expresses the belief that the Internet content is unsuited to copyright and other proprietary restraints. In 1996, John Perry Barlow, an early Internet pioneer and co-founder of the Electronic Frontier Foundation, reiterated this philosophy by proclaiming in his "Declaration of Independence in Cyberspace": "Your legal concepts of property, expression, identity, movement, and content do not apply to us. They are based on matter. There is no matter here."

However, as with any other original work of authorship, most content found on the Internet is protected by copyright. This includes software, images, text, videos, music, charts, diagrams, as well as postings to social media and blogs. None of these are automatically in the public domain merely because they are posted or displayed online. Copyright protection extends to expressions, including computer programs, but not to ideas, procedures, methods of operation, or mathematical concepts.

According to the Trade-Related Aspects of Intellectual Property Agreement (TRIPS), binding on all member countries of the World Trade Organization, the minimum term of protection is the life of the author plus no less than 50 years, although some members, like the United States and the European Union countries, extend the post mortem term to 70 years. When the copyright term expires, the work enters the public domain, which means that it is free for anyone to use. Alternatively, some authors choose to dedicate their work to the public domain. By doing so, they renounce any right to collect royalties when others use the work. There are several cooperative models that allow authors to surrender certain rights or license their content with few or no limitations, such as the Creative Commons network and the open source movement for software.

Truth: Most content on the Internet is protected by copyright and is not in the public domain or free to use, copy, adapt, or publicly display, perform, or distribute without a license from the copyright owner. Only when the author dedicates the work to the public domain is the content free to use without liability for infringement.

Source

Understanding Copyright and Related Rights, World Intellectual Property Organization (2016), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf; Kurt M. Saunders, Intellectual Property Law: Legal Aspects of Innovation and Competition (St. Paul, MN: West Academic, 2016).

MYTH #09

Im Internet ist alles gratis.

Nein, sagt Kurt M. Saunders: Die meisten Inhalte im Internet sind urheberrechtlich geschützt und weder gemeinfrei noch können sie ohne Genehmigung des Urheberrechtsinhabers frei genutzt, kopiert, geändert oder öffentlich angezeigt, aufgeführt oder verteilt werden. Nur wenn die Autor*innen das Werk der Öffentlichkeit zur Verfügung stellen, sind die Inhalte frei und ohne Verstoß gegen das Urheberrecht nutzbar.

كل شيء مجاني على الإنترنت.

كلا، هكذا يقول كيرت إم سوندرز: معظم محتوى الإنترنت محمي بموجب حقوق الطبع والنشر ولا يندرج ضمن المجال العام وليس مجانيّ الاستخدام أو النسخ أو الاقتباس أو العرض العام أو الأداء أو التوزيع دون رخصة من مالك حقوق الطبع والنشر. ولا يكون المحتوى مجانيّ الاستخدام إلا عندما يكرس المؤلف العمل للملك العام دون ترتب مسؤولية قانونية على الانتهاك.

在互联网上，一切都是免费的。

不，Kurt M. Saunders 写道： 互联网上的大部分内容受版权保护，未经版权所有人许可，不得在公有领域免费使用、复制、修改或公开展示、执行或分发其内容。 只有当作者将作品贡献至公有领域时，方可免费使用该内容，且无需承担侵权责任。

Sur Internet, tout est gratuit.

Non, écrit Kurt M. Saunders: la plupart des contenus sur Internet sont protégés par des droits d‘auteur et ne sont pas du domaine public, ni libres de droits d‘utilisation, de copie, d‘adaptation, de diffusion, de présentation ou de distribution publique sans obtention d‘une licence de détenteur de ces droits. Ce n’est que lorsque l’auteur dédie l’œuvre au domaine public que le contenu est libre d’utilisation, sans engagement de responsabilité en cas de violation.

В Интернете все доступно.

Это не так, говорит Курт М. Сондерс: Большинство контента в Интернете защищено авторским правом и не является общественным достоянием, не может безвозмездно использоваться, копироваться, изменяться, публично выставляться, демонстрироваться или распространяться без разрешения обладателя авторских прав. Только когда автор сделает свою работу достоянием общественности ее можно будет свободно использовать, не опасаясь ответственности за нарушение авторских прав.

Todo es gratis en el internet.

No, dice Kurt M. Saunders: la mayor parte del contenido en el internet está protegido por derechos de autor y no es de dominio público ni libre de usar, copiar, adaptar o exhibir, interpretar o distribuir públicamente sin una licencia del propietario de dichos derechos. Solo si el autor dedica la obra al dominio público, el contenido podrá ser libre de usar sin posibilidad de pena por infracción.

CHAPTER 2

Security and Safety

Schutz und Sicherheit

الأمن والسلامة

安全与保障

Sûreté et sécurité

Безопасность и защита

Seguridad y protección

MYTH #10

Matthias Schulze

Cyberwar is coming.

Myth: Cyber wars are inevitable. Modern economies are highly dependent on computers, which are vulnerable to hacking. A strategic cyber attack against a critical infrastructure, a power grid for example, thus could cripple an entire economy and could lead to mass-casualties. It is not a matter of if, but when such a scenario will occur.

Busted: In 1991 the threat of a digital pearl harbor, a surprise cyber attack targeting the strategic functions of a nation-state and thus crippling an entire economy, was conceived of for the first time. Since then we have heard that "cyberwar is coming!", because the transnational nature of the digital battlefield allows an attacker to strike from anywhere, anytime. It is not a matter of if, but when such a crippling cyber-attack would occur (Arquilla and Ronfeldt 1993). This cyber-doomsday scenario has been evoked repeatedly and features prominently in cyber strategies worldwide. (→ #13)

Although millions of different types of "cyber attacks" happen in any given year, only a handful of them have ever produced a kinetic effect (CFR Cyber Operations Tracker 2019). To this day, no one ever died as a direct result of a cyber attack. Stuxnet, the sabotage of Iranian nuclear enrichment centrifuges in 2010, still is the most extreme case. The two publicly known examples of a power-grid shut down in Ukraine 2016/2017 only lasted a couple of hours. Cyber attackers against power-plants usually do not disrupt operations, but rather install backdoors that can be utilized in a future conflict.

The strategic cyber war myth is based on a misunderstanding of the function of war and cyber capabilities. As von Clausewitz wrote, "war is [...] an act of violence intended to compel our opponent to fulfill our will". Most cyber attacks do not fit into the category of war, since they are not violent and often driven by financial, not political motives. Cyber espionage happens frequently, but lacks the motive of coercion (Rid 2013). We also confuse the possibility of a strategic cyber attack with its probability: such a scenario is possible, but improbable. The reason is that not much can be politically gained by such an attack out of the blue, unless its effects are made permanent with the use of physical force. Most cyber-attacks have temporary-disruptive, rather than permanent-destructive effects. This means that they cannot be used effectively to subdue or coerce an enemy in the same way as physical forces can: by occupying territory and permanently degrading enemy forces (Gartzke 2013). This explains why cyber-capabilities are mostly used as an adjunct to traditional, physical conflicts and not as a standalone feature. Only in these contexts something can be gained politically by using cyber-attacks - which is a core function of war as the continuation of politics by other means.

Truth: Many cyber strategies warn against the threat of a digital Pearl Harbor, a strategic cyber attack that could knock out the power grid and shut down an entire industrial economy. Although it is possible to shut down a power-grid from afar, not much can be gained politically by that, unless such a cyber-attack occurs within the context of a traditional, physical conflict, where the effect of such an attack can be made permanent. Cyber capabilities are used as tools in physical conflicts, but a standalone, digital-only strategic cyber war will not take place.

Source
Thomas Rid, Cyber war will not take place (London: Hurst, 2013); Brandon Valeriano and Ryan C. Maness, Cyber War versus Cyber Realities (Oxford: OUP, 2015)

MYTH #10

Der Cyberkrieg kommt.

Nein, sagt Matthias Schulze: Viele Cyberstrategien warnen vor der Bedrohung durch ein digitales „Pearl Harbor“, einen strategischen Cyberangriff, der Stromnetze sabotieren und die Volkswirtschaft einer ganzen Industrienation zum Erliegen bringen könnte. Zwar kann ein Stromnetz auch aus der Ferne abgeschaltet werden, jedoch kann daraus nur dann ein wesentlicher politischer Nutzen gezogen werden, wenn der Cyberangriff im Rahmen eines konventionellen physischen Konflikts erfolgt, bei dem die Wirkung des Angriffs verstetigt werden kann. Cyberfähigkeiten werden als ein Werkzeug in physischen Konflikten eingesetzt, jedoch wird ein eigenständiger, rein digitaler strategischer Cyberkrieg nicht stattfinden.

الحرب السيبرانية قادمة.

كلا، هكذا يقول ماتياس شولتسه: هناك الكثير من الاستراتيجيات السيبرانية التي تحذر من تهديد رقمي مشابه لـ «بيرل هاربور»، بمعنى هجوم إلكتروني استراتيجي يمكنه تعطيل شبكة الكهرباء وإصابة الاقتصاد الصناعي بأكمله بالشلل. وعلى الرغم من إمكانية تعطيل شبكة الكهرباء عن بُعد، إلا أنه لا يمكن تحقيق الكثير من المكاسب السياسية من وراء ذلك ما لم يحدث هذا الهجوم السيبراني في سياق صراع مادي تقليدي، حيث يمكن إسباغ صفة الديمومة عليه. وتُستخدم القدرات السيبرانية كأدوات في الصراعات المادية لكن لن تقع حرب سيبرانية رقمية مستقلة.

网络战即将到来。

不，Matthias Schulze 写道：许多网络战略都警告数字领域可能存在珍珠港偷袭式的威胁，即一场可能摧毁电网并关闭整个产业经济的战略性网络攻击。 虽然可以远程关闭电网，但这种做法在政治上无法取得太多收获，除非这种网络攻击发生在传统的物理冲突背景下，且会产生永久性影响。网络能力会被用作物理冲突中的工具，但不会发生单独的数字化战略网络战。

La cyberguerre est en marche.

Non, écrit Matthias Schulze : de nombreuses cyber-stratégies mettent en garde contre la menace d‘un Pearl Harbor numérique, une cyberattaque stratégique qui pourrait mettre le réseau électrique hors service et bloquer toute une économie industrielle. Bien qu’il soit possible de couper un réseau électrique à distance, on ne peut en tirer un grand avantage politique, à moins que cette cyberattaque ne se produise dans le contexte d’un conflit physique classique, conditions dans lesquelles les effets d’une telle attaque pourraient être rendus permanents. Les cyber-capacités sont utilisées comme outils dans le cadre de conflits physiques, mais une cyberguerre stratégique exclusivement numérique n‘est pas à craindre.

Грядет кибервойна.

Это не так, говорит Матиас Шульце: Многие киберстратегии предостерегают от угрозы «цифрового Перл-Харбора», стратегической кибератаки, которая может вывести из строя энергосистему и парализовать всю промышленную экономику. Несмотря на возможность удаленно вывести энергосистему из строя, в политическом плане это мало что даст, разве что такая кибератака произойдет в контексте традиционного физического конфликта, при котором результат такой атаки можно сделать постоянным. Киберинструменты используются в физических конфликтах, но автономная стратегическая кибервойна, где задействованы лишь цифровые технологии, не состоится.

Se avecina una guerra informática.

No, dice Matthias Schulze: diversas ciberestrategias advierten sobre la posibilidad de un Pearl Harbor digital, un ciberataque estratégico capaz de inhabilitar toda la red eléctrica y poner fuera de funcionamiento a toda una economía industrial. A pesar de que es posible inhabilitar una red eléctrica a distancia, no hay mucho que pueda ganarse de ello a nivel político, a menos que el ciberataque ocurriera en el contexto de un conflicto tradicional (físico), en el que los efectos de dicho ataque pudieran volverse permanentes. Las habilidades digitales son utilizadas como herramientas en el marco de conflictos físicos, pero una “ciberguerra”, con estrategias puramente digitales, no ocurrirá.

MYTH
#11

Thomas Reinhold

Arms control in cyberspace is not possible.

Myth: Arms control as an essential part of international peace and security-building is not applicable to cyberspace. This domain follows rules that differ strongly from air, sea, land and space. Therefore all established concepts of international security and the lessons learned from other military technologies cannot be applied to the Internet and any attempt to establish an arms control regime for cyber weapons is doomed to fail.

Busted: With Stuxnet, a malware that was targeted at a nuclear facility in Iran and detected in 2010, the international community realized that there are states which use cyberspace as the next domain for intelligence gathering and military purposes. (→ #10) This raised concerns that states could use cyber weapons to disrupt or destroy IT systems, worries that were confirmed by a 2013 report by the UN Disarmament Research Institute.

International policy-makers started to question how rules of arms control that had been developed over the last decades to restrict the usage and destructive effects of other weaponizable technologies and regulate their production or trade can be made to fit cyberspace. Early normative approaches like the Wassenaar Arrangement, a trade and export treaty, are appropriate for international trust building but limited in their impact on reducing arms races and the escalation potential between conflicting nations. Cyberspace with its characteristics of instantaneity, non-materiality and the possibility to seamlessly copy code and data undermines these approaches. You can see tanks massing at the border; it is much more difficult to see malware being prepared for attacks.

But Internet-based security challenges are critical for the private sector as well. Computer scientists and commercial companies have been developing approaches to fight cyber-weapons targeted at them for a long time. These approaches can be translated to calm the cyber arms race. An example of this is digital goods like songs which are as copyable as anything else in cyberspace. Nevertheless, companies have introduced digital rights management measures. Even if these are not always as effective as intended, this basically is, in arms control terminology, a regulation of proliferation. Other examples are Blockchain mechanisms for digital, tamper proof logs of information, the IPv6 mechanism for a worldwide unique identification of any device in cyberspace or the Border Gateway Protocol that enables data transfer across national IT networks and implements the traditional concept of borders. Many of these approaches, following the dual use logic in a non-traditional way, can be successfully applied to arms control in cyberspace.

Truth: Cyberspace is a human-made domain. While there are no specific cyberarms-oriented regulations or treaties, many approaches developed by computer scientists for ensuring cybersecurity and defending against cyberattacks in the offline world can be applied to cyberspace. Cyberarms control is possible, but it is necessary to go beyond existing normative approaches and sensibly adapt them.

Source

Thomas Reinhold and Christian Reuter, Arms Control and its Applicability to Cyberspace, in Christian Reuter (ed.), Information Technology for Peace and Security (Wiesbaden: Springer, 2019), 207–231

MYTH #11

Rüstungskontrolle ist im Cyberspace nicht möglich.

Nein, sagt Thomas Reinhold: Der Cyberspace ist ein vom Menschen geschaffenes Gebiet. Zwar existieren keine cyberwaffenspezifischen Regelungen oder Verträge, jedoch lassen sich viele Konzepte zur Gewährleistung von Cybersicherheit und zum Schutz vor Angriffen in der Offlinewelt auch auf den Cyberspace anwenden. Cyberrüstungskontrolle ist möglich, muss jedoch über bestehende normative Ansätze hinausgehen und diese sinnvoll adaptieren.

تحديد الأسلحة في الفضاء السيبراني ليس ممكنًا.

كلا، هكذا يقول توماس راينهولد: الفضاء السيبراني مجال من صُنع الإنسان. على الرغم من عدم وجود لوائح تنظيمية أو معاهدات محددة تستهدف الأسلحة السيبرانية إلا أن هناك الكثير من النُّهج التي طورها علماء الكمبيوتر لضمان الأمن السيبراني والدفاع ضد الهجمات السيبرانية في العالم غير الإنترنتي التي يمكن تطبيقها على الفضاء السيبراني. ويعتبر تحديد الأسلحة السيبرانية ممكنًا لكن يلزم تجاوُز حدود النُّهج المعيارية الحالية وتكييفها بشكل معقول.

网络空间无法实现军备控制。

不，Thomas Reinhold 写道：网络空间是一个人造领域。虽然没有以军备为导向的具体网络法规或条约，但计算机科学家为确保网络安全和防御线下世界的网络攻击而开发的许多方法均可应用于网络空间。网络军备控制有可能实现，但需要超越现有的规范方法并合理地进行调整。

Il n’est pas possible de contrôler les armes dans le cyberespace.

Non, écrit Thomas Reinhold: le cyberespace est une zone créée par l‘homme. Bien qu’il n’existe pas de réglementation ou de traité spécifiques en matière d‘armes sur Internet, de nombreuses approches développées par des informaticiens pour garantir la cybersécurité et se défendre contre les cyberattaques dans le monde hors ligne peuvent être appliquées au cyberespace. Le contrôle des armes est possible sur Internet, mais il est nécessaire d‘aller au-delà des approches normatives existantes et de les adapter de manière pragmatique.

Контроль над оружием в киберпространстве получить невозможно.

Это не так, говорит Томас Рейнхолд: Киберпространство создано человеком. Несмотря на отсутствие конкретных норм или соглашений в отношении кибероружия, многие разработанные программистами подходы по обеспечению кибербезопасности и защите от кибератак в реальном мире, могут применяться и к киберпространству. Контроль над кибероружием получить возможно, но необходимо выйти за рамки существующих нормативных подходов и рационально адаптировать их.

El control armamentístico no es posible en el ciberespacio.

No, dice Thomas Reinhold: el ciberespacio es un entorno creado por humanos. Si bien no hay tratados o regulaciones específicas relativos a las armas digitales, diversos enfoques desarrollados por científicos informáticos en temas de seguridad digital y defensa contra ciberataques en el mundo offline pueden ser aplicados al ciberespacio. El control de armas digitales es posible, pero es necesario ir más allá de los enfoques normativos existentes y adaptarlos de forma consecuente.

MYTH #12

Sven Herpig

The best cyber defense is a good cyber offense.

Myth: The offensive use of cyber capabilities as a response to cyber attacks carried out by an adversary (sometimes referred to as "hackbacks") deters criminals and state(-backed) actors and therefore increases security for your government, businesses, critical infrastructures and citizens ("deterrence-by-punishment").

Busted: The United States is among the leading countries when it comes to conducting offensive cyber operations with the ultimate goal to deter adversaries. Offensive use of cyber capabilities is one of many options when deciding how to respond to cyber operations. There are also political sanctions, economic sanctions, clandestine operations, military operations, criminal indictments and targeted financial sanctions against individuals.

If deterrence-by-punishment worked, there should be a significant drop in cyber operations against the United States. However, so far, large-scale data breaches and other cyber operations (DNC, F-35 stealth fighter blueprints, OPM, Equifax) continue to plague the United States. Because this strategy does not seem to work, the US government has shifted its approach from trying to deter an adversary through cyber means to conducting cyber operations to preempt adversarial cyber operations before they even happen under the new strategic doctrines of "defending forward" and "persistent engagement".

In addition to the apparent failure of deterrence-by-punishment, immediate offensive countermeasures to disrupt ongoing attacks or retrieve "stolen" data, so-called "hackbacks", face tremendous challenges. Attributing an attack and responding in time without any prior preparations (e.g. carefully scanning for/compromising vulnerable systems) is nearly impossible. Such a strategy would therefore rather lead to more IT insecurities as it requires the responsible agencies to stockpile vulnerabilities and hack tools without a decent chance of successfully using them.

With few exceptions, such as the allegedly US-Israel cyber campaign against nuclear enrichment facilities in Iran (Stuxnet), cyber operations have not yet exceeded a certain threshold and might therefore currently be at the lower end of an escalation cycle. Other responses, such as sanctions and indictments, might be more proportionate and effective and therefore will yield better results in fighting the adversary off. There is however no solid data substantiating that any of those response strategies achieves any lasting (deterring) effect.

There is simply no proof that offensive cyber defense works. The United States as the key actor has shifted its strategy from deterring to preempting cyber operations. Attribution of cyber operations continues to be a major challenge. Forensic analysis of attacks takes time and attributions and actors increasingly use malicious software stitched together from the code of other threat actors (Vault7) to conduct false-flag operations. If attribution continues to be a major challenge, attackers will be unlikely to be deterred because they can be confident that they will remain anonymous.

Truth: The use or threat of preemptive offensive cyber capabilities does not deter adversaries from attacking you. The use of better IT security and resilience mechanisms might also not deter them ("deterrence-by-denial"), but will decrease the likelihood that they succeed and therefore increase security for your government, businesses, critical infrastructures and citizens.

Source

Sven Herpig, Anti-War and the Cyber Triangle: Strategic Implications of Cyber Operations and Cyber Security for the State, PhD thesis, University of Hull (2015); Sven Herpig and Thomas Reinhold, Spotting the bear: credible attribution and Russian operations in cyberspace, Chaillot Paper 148 (2018), 33–42

MYTH #12

Die beste Cyberverteidigung ist ein guter Cyberangriff.

Nein, sagt Sven Herpig: Der Einsatz oder die Androhung präventiver, offensiver Cyberfähigkeiten hindert den Gegner nicht daran anzugreifen. Der Einsatz besserer IT-Sicherheits und Resilienzmechanismen hat nicht unbedingt abschreckende Wirkung („Abschreckung durch Zugangsverweigerung“), verringert jedoch die Erfolgswahrscheinlichkeit des gegnerischen Angriffs und erhöht somit die Sicherheit für Regierungen, Unternehmen, kritische Infrastrukturen und Bürger*innen.

أفضل دفاع سيبراني هو الهجوم السيبراني الجيد.

كلا، هكذا يقول سفين هيربيغ: إن استخدام أو التهديد باستخدام القدرات السيبرانية الهجومية الاستباقية لا يردع الخصوم عن مهاجمتك. وقد لا يردعهم أيضًا استخدام آليات أفضل لأمن تكنولوجيا المعلومات والقدرة على الصمود («الردع بالتلويح بالخسارة»)، لكنه سيُقلل من احتمالية نجاحهم وبالتالي يزيد أمن حكومتك وشركاتك وبناك التحتية الحيوية ومواطنيك.

最佳的网络防御就是良好的网络攻击。

不，Sven Herpig 写道：先发制人的攻击性网络能力的使用或威胁并不能阻止对手攻击您。使用更好的 IT 安全和弹性机制仍可能无法阻止对手进行攻击（“拒止性威慑”），但会降低攻击成功的可能性，提高政府、企业、主要基础设施和公民的安全。

La meilleure cyberdéfense est une bonne cyberattaque.

Non, écrit Sven Herpig : l’utilisation ou la menace de cyber-capacités offensives préventives ne dissuade pas les adversaires de vous attaquer. L‘utilisation de meilleurs mécanismes de sécurité et de résilience informatiques pourrait également ne pas suffire à les dissuader (« dissuasion par déni »), mais cela diminuerait leurs chances de réussite et augmenterait donc la sécurité de votre gouvernement, de vos entreprises, de vos infrastructures critiques et de vos citoyens.

Лучшая киберзащита – это кибернападение.

Это не так, говорит Свен Херпиг: Использование или угроза предупредительных наступательных кибер-возможностей не сдерживает противников от нападения на вас. Использование более эффективных механизмов информационной безопасности и стойкости также не остановит их («сдерживание воспрещением»), но снизит вероятность того, что они добьются успеха и, следовательно, повысит безопасность вашего правительства, предприятий, ключевой инфраструктуры и граждан.

La mejor ciberdefensa es un buen ciberataque.

No, dice Sven Herpig: el uso o la amenaza de usar las capacidades digitales ofensivas a modo preventivo no disuade a sus adversarios de atacarlo. La aplicación de mecanismos de seguridad y resiliencia informática más efectivos tampoco los disuadirá (“disuasión por negación”), pero sí disminuirá sus probabilidades de éxito y por lo tanto aumentará la seguridad de su gobierno, empresa, infraestructuras críticas y ciudadanos.

MYTH #13

Andrew Odlyzko

Drastic improvements in cybersecurity are urgently needed.

Myth: The Internet and all other information systems need to be re-engineered from the ground up to provide robust security. Failure to do so will expose society to rapidly escalating financial losses, as well as greater erosion of privacy and a corrosive “post-truth” environment, and might end in a “digital Pearl Harbor” that could bring the economy to a halt.

Busted: Cyber risks are real and are growing. (→ #10) But they are not much different from the threats in the physical world and are similarly manageable. They have been managed in the past, and that experience of living with and depending on obviously insecure systems over several decades provides useful lessons for the future.

We have learned that we cannot build secure systems of substantial complexity. Even if we could, human vulnerabilities that are exploited so effectively through techniques such as phishing would remain. However, in the past the damage from lack of cyber security has been tolerable, typically less than from other forms of crime, natural disasters, and innocent bugs or operational errors. The key issue has always been risk management, not absolute security, just as in the physical world. This is because security is not the paramount goal and only a certain level of it is necessary to allow individuals and organizations to function and flourish.

An instructive example is that of two-factor authentication. It has been known and available commercially for about three decades, but it is only now becoming widely deployed. Clearly organizations decided in the past it was not worth using it. And, in retrospect, it is hard to argue this decision was incorrect. An even more obvious example is that of rigorous observation of standard security practices (prompt application of updates, use of secure passwords, and the like). It is standard, and is universally accepted as desirable, but is seldom followed. If necessary, security could be increased by simply adhering to those standards.

There is of course the threat of a large scale cyber attack. (→ #12) Experience indicates that such could realistically only be mounted by large state actors. Hence they have to be deterred by government agencies and so hopefully will not be much more of a threat than giant geomagnetic storms.

For most individuals and organizations, the only serious worry should be routine criminal attacks. Protection against those can be improved in various simple ways. Among the most important of those ways is providing secure backups and engineering systems for quick recovery. Such measures would also provide protection against large scale attacks.

Truth: We are not facing a cybersecurity crisis, and there is no need for a fundamental re-engineering of our information systems. Cyberthreats are mounting, but in a measured way, and we already have many tools for strengthening our security. Hence we are likely to provide adequate levels of security by acting as before, taking small incremental steps as necessary

Source

Andrew Odlyzko, Cybersecurity is not very important, ACM Ubiquity, June 2019, 1–23, https://ubiquity.acm.org/article.cfm?id=3333611.

MYTH #13

Drastische Verbesserungen der Cybersicherheit sind dringend erforderlich.

Nein, sagt Andrew Odlyzko: Wir stehen nicht vor einer Cybersicherheitskrise und es besteht keine Notwendigkeit für eine grundlegende Umgestaltung unserer Informationssysteme. Cyberbedrohungen nehmen zu, aber auf beherrschbare Weise, und es stehen bereits etliche Werkzeuge zur Verbesserung unserer Sicherheit zur Verfügung. Es ist daher wahrscheinlich, dass wir ein angemessenes Maß an Sicherheit garantieren können, wenn wir wie bisher handeln und nur bei Bedarf geeignete Maßnahmen setzen.

هناك حاجة مُلحَّة إلى تحسينات جذرية في الأمن السيبراني.

كلا، هكذا يقول أندرو أودليزكو: لسنا في مواجهة أزمة أمن سيبراني، ولا حاجة إلى عملية إعادة هندسة جذرية لنظم معلوماتنا. إن التهديدات السيبرانية في تصاعُد لكن بطريقة متروّية، ولدينا بالفعل العديد من الأدوات لتعزيز أمننا. وبالتالي فالمرجح أن نوفر مستويات كافية من الأمن من خلال متابعة عملنا بنفس النهج السابق، مع اتخاذ خطوات إضافية صغيرة حسب الحاجة.

迫切需要在网络安全方面取得重大进展。

不，Andrew Odlyzko 写道：我们尚未面临网络安全危机，也没有必要对我们的信息系统进行根本性的重建。网络威胁正有规律地日益增加，但我们已经有很多工具来加强我们的安全。因此，我们可能会像以前一样提供足够的安全保障，并在必要时采取逐渐增加的措施。

Des améliorations drastiques de la cybersécurité sont nécessaires de toute urgence.

Non, écrit Andrew Odlyzko : nous ne vivons pas de crise de cybersécurité, une réorganisation en profondeur de nos systèmes d‘information n‘est pas nécessaire. Les cybermenaces augmentent, mais de manière mesurée, et nous disposons déjà de nombreux outils pour renforcer notre sécurité. Il est donc probable que nous puissions garantir des niveaux de sécurité adéquats en agissant comme nous le faisons déjà, en prenant de petites mesures supplémentaires au besoin.

Необходимо принять неотложные меры по усилению кибербезопасности.

Это не так, говорит Эндрю Одлызко: Мы не переживаем кризис кибербезопасности, поэтому нет необходимости в фундаментальной реорганизации наших информационных систем. Киберугрозы растут в умеренном темпе, к тому же у нас уже есть множество инструментов для укрепления нашей безопасности. А значит мы способны обеспечить должный уровень безопасности, действуя так же, как и раньше, постепенно предпринимая небольшие шаги по мере необходимости.

Se requieren mejoras drásticas urgentes en materia de ciberseguridad.

No, dice Andrew Odlyzko: no estamos afrontando una crisis de ciberseguridad y no hay necesidad de una reestructuración radical de nuestros sistemas informáticos. Las amenazas digitales van en aumento, pero de forma mesurada, y disponemos ya de numerosas herramientas para aumentar nuestra protección. Por lo tanto, es probable que mantengamos niveles adecuados de seguridad si seguimos actuando como lo hemos hecho hasta ahora, dando pequeños pasos graduales según sea necesario.

MYTH #14

Thorsten Thiel

Only criminals want anonymity online.

Myth: Digital communication furthers anonymous communication and being anonymous makes people behave unaccountably and irresponsibly, erodes societal trust and has a deleterious effect on the public discourse. Anonymity is an unfair opportunity to take advantage of others, spread hate or commit crimes. Therefore, it should be outlawed.

Busted: It is often assumed that the rise of networked communication has made the world more anonymous. (→ #5) This is false or at least needs to be substantially qualified. While computer-mediated communication always works in a somewhat pseudonymous way and it is certainly possible to hide one's identity vis-à-vis other Internet users in most circumstances, the ability of resourceful actors like states and corporate entities to identify and track users has significantly increased. Digital communications can be held, tracked and analyzed - and the possibilities to re-identify persons have been vastly improved to the detriment of fundamental rights. Staying anonymous in a data-rich environment is something demanding that must be actively sought. The starting point of the argument is, therefore, wrong.

Secondly, anonymity does not only benefit criminals (although they too might make use of anonymization techniques). Anonymity is vital to many different individuals or groups in society. Minorities or political activists are a prime example since they often need a secure space to find and form their identity and debate how to position towards the wider society. (→ #18) There are also many professional groups in society – think of journalists, therapists, etc. – that are dependent on contexts where anonymity can be safely assumed and actively protected. Finally, individuals themselves may benefit from a societal structure that sets anonymous communication as the default. Anonymity allows citizens to try out different identities (and, thereby, learn about the views of others), to change opinions over time and to speak their mind. Not being observable is an important good in a liberal society - for reasons of privacy as well as democracy. (→ #17)

Furthermore, anonymity does not in itself trigger bad or irresponsible behaviour. Empirical studies show that there is no clear case to be made that people who communicate anonymously behave worse than people who are knowingly identifiable. Much depends on the context, cultural factors and the inclinations of the actors. Anonymity might also yield a more open and creative behaviour, counter biases or inspire an equal discourse instead of a shallow and conformist reputation management.

Truth: Since identification possibilities are ubiquitous and pervasive, it is no longer enough to just tolerate pseudonymity online. Instead, we have to find ways to ensure that also in the digital constellation anonymity is actively preserved in the sense that at least in certain specified contexts anonymity is legally secured and technologically assisted. A broad, but measured societal discourse on the benefits and risks of anonymous communication is key to achieve this.

Source

Hans Asenbaum, Anonymity and Democracy: Absence as Presence in the Public Sphere, American Political Science Review 112 (2018): 1–14; Gary T. Marx, What's in a Name? Some Reflections on the Sociology of Anonymity, The Information Society 15 (1999), 99–112

MYTH #14

Nur Kriminelle wollen Anonymität im Internet.

Nein, sagt Thorsten Thiel: Anonymität ist ein zunehmend rares Gut in der vernetzten Gesellschaft, sollte jedoch aktiv geschützt werden, da sie vielen Menschen und Gruppen in der Gesellschaft erlaubt, ihre Stimme zu erheben. Anonymität per se führt nicht zu verwerflichem Verhalten. Liberale Gesellschaften sollten gesellschaftliche Kontexte diskutieren und definieren, in denen anonyme Kommunikation akzeptiert und geschützt wird.

المجرمون وحدهم يريدون خفاء الهوية على الإنترنت.

كلا، هكذا يقول تورستن تيل: خفاء الهوية هو أحد الحسنات الآخذة في التلاشي في المجتمع الشبكي، لكنه أمر ينبغي أن نسعى جاهدين للحفاظ عليه لأنه يساعد الكثير من الأفراد والفئات في المجتمع على إيجاد فرصة للتعبير عن آرائهم. ولا يؤدي خفاء الهوية في حد ذاته إلى سلوك سيئ. وينبغي على المجتمعات الليبرالية أن تناقش وتحدد السياقات الاجتماعية التي يُقبل فيها الاتصال مجهول الهوية ويكون مؤمنًا.

只有罪犯想要在网络上匿名。

不，Thorsten Thiel 写道：匿名是网络社会中即将消失的益处，我们应积极保留，因为它可以帮助社会中的许多个人和群体发出自己的声音。匿名本身并不会造成不良行为。自由社会应该讨论和定义接受并保护匿名通信的社会背景。

Seuls les criminels veulent l‘anonymat en ligne.

Non, écrit Thorsten Thiel : l‘anonymat est un bien en voie de disparition dans la société en réseau, mais il convient de le préserver activement, car il aide de nombreux individus et groupes à pouvoir avoir la parole dans nos sociétés. L‘anonymat en soi ne conduit pas à de mauvais comportements. Les sociétés libérales devraient débattre et définir des contextes sociétaires dans lesquels la communication anonyme est acceptée et sécurisée.

Только преступники хотят сохранить анонимность в Интернете.

Это не так, говорит Торстен Тиль: Анонимность – это исчезающее благо в сетевом обществе. Иногда ее следует активно сохранять, поскольку она помогает многим людям и группам в обществе обрести свой голос. Анонимность сама по себе не подталкивает к плохому поведению. Либеральным обществам следует обсудить и установить социальный контекст, в котором анонимное общение будет общепризнанно и защищено.

Solo los criminales desean el anonimato en el internet.

No, dice Thorsten Thiel: el anonimato es un bien que escasea cada vez más en nuestras sociedades interconectadas, sin embargo es algo que deberíamos intentar preservar activamente, ya que ayuda a muchos individuos y grupos de la sociedad a tener una voz. El anonimato por sí mismo no lleva al mal comportamiento. Las sociedades liberales deberían debatir y definir contextos sociales en los que la comunicación anónima sea aceptada y protegida.

MYTH #15

Ian Peter

The Internet was invented by the Pentagon and designed to survive a nuclear attack.

Myth: Fuelled largely by the early writings of Silicon Valley gossip columnist Robert Cringely in the early 1990s, a popular belief has sprung up that the Internet was invented in the Pentagon in 1969 and was designed to survive a nuclear attack. In fact, this assumption is so widespread that you could call it "the big bang theory of Internet origins".

Busted: It's not surprising that people began to believe that, in a Cold War scenario, a project of the Defence Advanced Research Projects Agency (DARPA) would have a military purpose. But in fact that was not the case with Arpanet, which was essentially established for a purely functional computing science purpose of allowing mainframe computers (military or otherwise) to communicate with each other. It was all about finding a way to share data between disparate systems.

The facts about Arpanet come from the person who was in charge of the project from its inception in 1966 until late 1969, Bob Taylor. To quote correspondence with him: "In February of 1966 I initiated the ARPAnet project. I was Director of ARPA's Information Processing Techniques Office (IPTO) from late ,65 to late ,69. There were only two people involved in the decision to launch the ARPAnet: my boss, the Director of ARPA Charles Herzfeld, and me. The creation of the ARPAnet was not motivated by considerations of war. The ARPAnet was created to enable folks with common interests to connect with one another through interactive computing even when widely separated by geography".

Despite a number of online exchanges with other people working on the ARPAnet project, this fact has not been disputed or challenged. So in fact Arpanet had nothing to do with nuclear war (except perhaps in a sense that better computing capabilities would enhance military capabilities). Arpanet was simply about trying to solve a common problem in those days – getting computers with disparate operating systems to communicate with each other. Similar efforts were under way in France (Louis Pouzin and the Cyclades Project) and United Kingdom (Donald Davies, National Physics Laboratory). From these sources came the concept of packet switching, which Arpanet adopted at a later stage as a way to transfer packets of data from one computer to another.

Later on, in 1973, another important addition to this work was the introduction of the TCP/IP transport protocol, invented by Vint Cerf and Bob Kahn. Other important early work was undertaken at Xerox Parc Laboratories by John Schoch and Robert Metcalfe. All of these developments came together to give us the early technical foundations of the Internet. Experts differ in their interpretations of the importance of these related developments and as to which (if any) can be considered to be the primary origins of the Internet.

Truth: Whatever role you wish to attribute to Arpanet as regards the origins of the Internet, it is clear that the early Internet was not motivated by considerations of nuclear war, but by a need for technical protocols to allow computers (and their users) to communicate. ARPAnet was primarily an early computing science exercise, rather than a military one.

Source

Robert Taylor and others (posted by Dave Farber), Dave Farber's Interesting People Mailing list (October 2004 archives), https://seclists.org/interesting-people/2004/Oct/index.html; Ian Peter, Internet History Site, https://www.nethistory.info.

MYTH #15

Das Internet wurde erfunden und so konzipiert, dass es einen Atomangriff übersteht.

Nein, sagt Ian Peter: Welche Rolle man ARPAnet auch immer hinsichtlich des Ursprungs des Internets zuweist, bleibt es eine Tatsache, dass die Entwicklung des frühen Internets nicht auf der Furcht vor einem Atomkrieg beruhte, sondern der Notwendigkeit technischer Protokolle für die Kommunikation zwischen Computern (und ihren Nutzer*innen) entstammt. ARPAnet war in erster Linie eine frühe wissenschaftliche Leistung auf dem Gebiet der Informatik und nicht ein Erfolg des Militärs.

اختُرعت الإنترنت وصُممت للنجاة من أي هجوم نووي.

كلا، هكذا يقول أيان بيتر: أياً كان الدور الذي ترغب في نسبته إلى «ARPAnet» فيما يتعلق بنشأة الإنترنت، فالواضح أن الإنترنت المبكرة لم تكن مدفوعة باعتبارات الحرب النووية، بل كانت مدفوعة بالحاجة إلى بروتوكولات فنية تسمح بالاتصال بين أجهزة الكمبيوتر (ومستخدميها). كانت «ARPAnet» في المقام الأول ممارسة مبكرة في علم الحوسبة لا ممارسة عسكرية.

互联网的发明和设计是为了躲过核攻击。

不，Ian Peter 写道：关于互联网的起源，不论您希望阿帕网 (ARPAnet) 扮演何种角色，很明显，早期的互联网并非出于核战争的考虑，而是出于允许计算机（及其用户）进行通信的技术网络协议的需要而出现的。阿帕网主要是早期的计算科学实验，而非军事实验。

Internet a été inventé et conçu pour survivre à une attaque nucléaire.

Non, écrit Ian Peter : quel que soit le rôle que vous souhaitiez attribuer à ARPAnet quant aux origines d’Internet, il est évident que la motivation première du premier Internet n’était pas une guerre nucléaire, mais plutôt le besoin de disposer de protocoles techniques permettant aux ordinateurs (et à leurs utilisateurs) de communiquer. ARPAnet était avant tout un exercice scientifique précoce, plutôt qu‘un exercice militaire.

Интернет был придуман и создан для того, чтобы пережить ядерную атаку.

Это не так, говорит Ян Питер: Какую бы роль вы ни приписывали ARPAnet относительно возникновения Интернета, очевидно, что причиной появления раннего Интернета послужила не ядерная война, а необходимость в технических протоколах, позволяющих компьютерам (и их пользователям) общаться. ARPAnet был в первую очередь ранним научным нежели военным экспериментом.

El internet fue inventado y diseñado para sobrevivir ataques nucleares.

No, dice Ian Peter: independientemente del rol que se desee atribuir al ARPAnet en relación con el origen del internet, queda claro que, en sus primeros años, el internet no estaba motivado por consideraciones de guerra nuclear, sino por una necesidad de protocolos técnicos que permitieran a las computadoras (y a sus usuarios) comunicarse entre sí. ARPAnet fue, por encima de todo, un experimento de ciencia computacional y no uno militar.

MYTH #16

Ilja Sperling

End-to-end encrypted messaging means that pure privacy is protected.

Myth: In an era where privacy is under a constant threat from state and non-state actors, people rely on end-to-end encrypted communication. Popular services such as WhatsApp, iMessage, or Telegram promise to protect our privacy and reassure us that our interactions are "secured from falling into the wrong hands".

Busted: End-to-end encryption (E2EE) is a strong promise which gives the user (and their peers) a false sense of security and privacy. While E2EE in itself is a great security paradigm, it is probably less obvious to users that the transmission of encrypted messages is not all but one part of the privacy equation. While law enforcement agencies or companies such as the NSO Group actively seek to exploit endpoint vulnerabilities, privacy is further undermined by incautious user behaviour (i.e. unprotected devices; unencrypted backups) and bad app designs (i.e. storing messages decrypted). (→ #45)

Here is one less obvious threat model: Have you ever used WhatsApp, Telegram, or iMessage to share an online news article, a Facebook post, or any website link in general? Have you ever wondered about the rendered preview of the content that you are sharing? Usually, it's an unobtrusive element, displaying the title, a teaser, the URL, and a thumbnail.

Well, this is indeed external content and your messaging app just fetched it from a remote server – without asking you for permission, masking your identity from a third party, and usually without offering you an opt-out. While link preview might appear convenient, it is a non-trivial threat to your privacy and to the privacy of the target of your encrypted message.

The most basic threat is that the link preview reveals your public IP address and your application's User-Agent to a third party (the content's host). While desktop email clients usually warn you when there is remote content, mobile messaging apps strangely don't. If you are merely one among millions of visitors of a website, this might not bother you. However, if you are an investigative journalist or a queer activist who is being targeted by a phishing campaign, you might conclude that your privacy has just been violated and that you have been invisibly put at risk by your messaging app.

There are several harmful scenarios where an actor with access to a server's logfile or an authoritarian regime capable of monitoring the network traffic can turn the link preview feature into a tool of targeted surveillance. How this can be done, has been shown by Justin Seitz (2019), who has documented the behaviour of various messaging apps for the investigative platform Bellingcat.

Truth: The link preview feature in popular end-to-end encrypted messaging apps such as WhatsApp, Telegram, or iMessage discloses your and your peer's identity to a third party. This is an even bigger problem for messaging tools without E2EE, such as Instagram or Slack. Malign actors can turn this privacy violation into a surveillance and tracking tool.

Source

Justin Seitz, How To Blow Your Online Cover With URL Previews, Bellingcat (2019), https://www.bellingcat.com/resources/how-tos/2019/01/04/how-to-blow-your-online-cover-with-url-previews; Justin Wu and Daniel Zappala, When is a Tree Really a Truck? Exploring Mental Models of Encryption, Fourteenth Symposium on Usable Privacy and Security, SOUPS (2018), https://www.usenix.org/conference/soups2018/presentation/wu.

MYTH #16

Ende-zu-Ende-verschlüsseltes Messaging garantiert perfekten Datenschutz.

Nein, sagt Ilja Sperling: Die Linkvorschaufunktion in beliebten Messaging-Apps mit Ende-zu-Ende-Verschlüsselung (E2EE) wie beispielsweise WhatsApp, Telegram oder iMessage gibt die Identität der Kommunikationspartner*innen an Dritte weiter. Noch schwerer wiegt dieses Problem bei Messaging-Tools ohne E2EE wie beispielsweise Instagram oder Slack. Es besteht die Möglichkeit, diesen Datenschutzeingriff zum Schaden von Nutzer*innen in ein Überwachungs und Verfolgungsinstrument zu verwandeln.

الرسائل المشفرة بين الطرفين تعني ضمان الخصوصية التامة.

كلا، هكذا يقول إيليا سبيرلينغ: تكشف خاصية معاينة الرابط في تطبيقات المراسلة المشفرة وفقاً لمبدأ الطرفين الشهيرة، مثل WhatsApp أو Telegram أو iMessage، عن هويتك وهوية نظيرك لطرف ثالث. والمشكلة أكبر بالنسبة لأدوات المراسلة التي تفتقر إلى التشفير وفقاً لمبدأ الطرفين، مثل Instagram أو Slack، حيث يمكن للأطراف سيئة النية تحويل انتهاك الخصوصية هذا إلى أداة للمراقبة والتتبع.

端到端加密通讯意味着纯隐私受到保护。

不，IIja Sperling 说道：流行的端到端加密通讯应用程序（如 WhatsApp, Telegram 或 iMessage）中的链接预览功能可向第三方披露您与您对等端的身份。对于没有端到端加密功能的通讯工具，例如 Instagram 或 Slack，这是个更大的问题。恶意行为者可将此隐私侵犯转变为监督和追踪工具。

échanger des messages chiffrés de bout en bout signifie que la confidentialité est protégée.

Non, dit Ilja Sperling: la fonction de prévisualisation de lien dans les applications de messagerie chiffrées de bout en bout les plus répandues, telles que WhatsApp, Telegram ou iMessage, divulgue votre identité et celle de votre correspondant à un tiers. Le problème est encore plus grand pour les outils de messagerie sans chiffrement (E2EE), tels qu'Instagram ou Slack. Les acteurs les plus sournois peuvent transformer cette violation de confidentialité en un outil de surveillance et de suivi.

Передача сообщений с применением сквозного шифрования обеспечивает сохранение абсолютной конфиденциальности.

Это не так, говорит Илья Сперлинг: Функция предварительного просмотра ссылок в популярных приложениях, таких как WhatsApp, Telegram или iMessage, где происходит передача сообщений с применением сквозного шифрования, раскрывает третьим лицам вашу личность, а также личность вашего собеседника. Это еще большая проблема в отношении таких инструментов, как Instagram или Slack, которые не используют сквозное шифрование для передачи сообщений. Злоумышленники могут превратить это нарушение конфиденциальности в инструмент наблюдения и отслеживания.

Los mensajes cifrados de extremo a extremo (E2EE) garantizan una protección de la privacidad.

No, dice Ilja Sperling: la función de vista previa de enlace de los servicios de mensajes cifrados populares, tales como WhatsApp, Telegram o iMessage, revela su identidad y la de su interlocutor a un tercero. Este problema es aún mayor en el caso de las herramientas de mensajes sin cifrado E2EE, tales como Instagram o Slack. Actores malintencionados pueden hacer de esta violación de la privacidad una herramienta de vigilancia y monitoreo.

MYTH #17

Suzette Leal

The dark web is a hidden place of evil.

Myth: The dark web is an expansive, impenetrable, invisible, immoral fantasyland of sexual child exploitation, terrorist organizations, data theft, and cryptocurrency-based drug deals. It is also at the core of the cyber threat economy, a place where hacking tools are traded to assault commercial organizations or individuals. Essentially, it is the source of everything digitally evil.

Busted: Even though the dark web enjoys more anonymity and freedom from censorship, it is not the online underworld where serious criminals roam free. (→ #14) Firstly, the dark web is certainly not impenetrable, and dubious content is not impossible to remove. Although surveillance of dark web content is more challenging, the mere trust factor that is required for any network to function renders the dark web fragile to the identification of criminals and illegal content. In this vein, a considerable part of the dark web is visible and relatively easy to connect with through forums and wikis. The dark web is also not the expansive iceberg it is portrayed to be – this huge underbelly of questionable online behaviour constituting most Internet activity. In fact, compared to surface web traffic, activities on the dark web is minimal.

Perhaps the most significant misconception regarding the dark web pertains to the general assumption that it is inherently dangerously corruptive. Terrorism and the sexual exploitation of children account for very little dark web activity. Furthermore, whilst it cannot be disputed that the dark web is a vessel for illegal activities such as human trafficking, fraud and drug deals, one should not underestimate the very role the regular Internet plays in such activities. In overestimating or even embellishing the power and mystery of the dark web, moral panics may lead to ill-directed government policies – ones that overlook illicit activities in obvious places.

In truth, as much as half of the dark web involves legitimate activities – content such as software repositories, and activism-related blogs and/or websites. A considerable number of dark web users are truly in need of anonymity, privacy and protection. In countries where Internet use is restricted, monitored and controlled, marginalized minorities such as the LGBT community often use the dark web to communicate, share ideas and express opinions. Journalists use the dark web to protect their sources, and media organizations host secure lockboxes on the dark web to guarantee safety and anonymity to whistleblowers. Freedom of expression is, in fact, often the overriding reason for engagement on the dark web with users exercising agency without any intent of harming or hurting others.

In essence, a layer of invisibility does not necessarily or automatically create deviance and misconduct. The dark web provides anonymity, and this is used for both good and, unfortunately, evil. One should however not allow “darkness of morality” to become the narrative associated with the dark web.

Truth: The dark web embraces all activity that cannot be searched or indexed using standard search engines. Although the anonymity and freedom associated with dark web also facilitate criminal activities, the dark web is not the epitome of mysterious, suspicious and illicit conducts. In fact, a significant portion of dark web activities is used to protect those who need privacy and to allow people under threat to communicate.

.

Source
Mihnea Mirea, Victoria Wang and Jeyong Jung. The Not So Dark Side of the Darknet: A Qualitative Study. Security Journal, 32(2) (2018), 102–118; Georgia Avarikioti, Roman Brunner, Aggelos Kiayias, Roger Wattenhofer and Dionysis Zindros. Structure and Content of the Visible Darknet, ArXiv (2018), 1811.01348(2)1–27.

MYTH
#17

Das Darknet ist ein verborgener Ort des Bösen.

Nein, sagt Suzette Leal: Das Darknet ist ein Ort für Aktivitäten, die nicht über Standardsuchmaschinen gefunden oder indexiert werden können. Auch wenn die mit dem Darknet einhergehende Anonymität und Freiheit das Begehen von Straftaten erleichtern mag, ist das Darknet dennoch nicht der Inbegriff für verdecktes, per se verdächtiges und zwingend rechtswidriges Verhalten. Ein erheblicher Teil der Aktivitäten im Darknet stellt die schwer zu überwachende Kommunikation zwischen bedrohten Nutzer*innen dar.

الشبكة المظلمة مكان خفي للأشرار.

كلا، هكذا تقول سوزيت ليال: تضم الشبكة المظلمة جميع الأنشطة التي لا يمكن البحث فيها أو فهرستها باستخدام محركات البحث الاعتيادية. وعلى الرغم من أن خفاء الهوية والحرية المرتبطين بالشبكة المظلمة يسهلان الأنشطة الإجرامية أيضًا، إلا أن الشبكة المظلمة ليست نموذجًا يجسد السلوك الغامض والمشبوه وغير المشروع. والواقع أن جزءًا كبيرًا من أنشطة الشبكة المظلمة يُستخدم لحماية من يحتاجون إلى الخصوصية وللسماح بتواصل الأشخاص المعرضين للتهديد.

暗网是隐藏的邪恶之地。

不，Suzette Leal 写道：暗网包含使用标准搜索引擎无法搜索或检索的所有活动。虽然与暗网有关的匿名和自由也会助长犯罪活动，但暗网并不是神秘、可疑和非法行为的缩影。事实上，暗网活动很大一部分用于保护需要隐私的人士以及允许受到威胁的人士进行通信。

Le dark web est la tanière du diable.

Non, écrit Suzette Leal : le dark web regroupe toutes les activités qui ne peuvent pas être recherchées ou indexées à l‘aide de moteurs de recherche standard. Bien que l‘anonymat et la liberté associés au dark web facilitent également les activités criminelles, ce n‘est pas l’épicentre de comportements mystérieux, suspects et illicites. En fait, une partie importante des activités se passant sur le dark web est utilisée pour protéger ceux qui ont besoin de confidentialité et pour permettre aux personnes menacées de communiquer.

Дакрнет – скрытый очаг зла.

Это не так, говорит Сюзетт Лил: Дакрнет включает все виды деятельности, которые нельзя отыскать или проиндексировать с помощью стандартных поисковых систем. Хотя анонимность и свобода, с которыми ассоциируется даркнет, также облегчают преступную деятельность, он не является воплощением таинственной, подозрительной и незаконной активности. Более того, значительная часть активности в даркнете направлена на защиту тех, кому нужна конфиденциальность, позволяя общаться тем, кому угрожает опасность.

El dark web es un lugar secreto de maldad.

No, dice Suzette Leal: el llamado dark web (internet oculto u oscuro) comprende toda la actividad que no puede ser encontrada o indexada utilizando los motores de búsqueda convencionales. Aunque es verdad que el anonimato y la libertad asociada al dark web facilita las actividades criminales, el dark web no representa en sí mismo un epítome de conducta anónima, sospechosa e ilícita. De hecho, una parte importante de las actividades del dark web sirve para proteger a aquellos que requieren de privacidad y para permitir comunicarse a las personas que se encuentran bajo amenaza.

CHAPTER 3

Inclusion and Integration

Inklusion und Integration

الإدماج والتكامل

包容与整合

Inclusion et intégration

Инклюзивность и интеграция

Inclusión e integración

MYTH #18

Katharina Mosene

The Internet is an emancipatory tool to end all discrimination.

Myth: The Internet and information and communication technologies are neutral tools providing public spaces that offer easy and effective participation for all and make so-called minority-issues part of a larger social discourse, thereby fostering inclusion and overcoming power differentials that plague traditional and linear media.

Busted: An end to sexism, racism, ableism? For a long time, the Internet was regarded as the foremost emancipatory tool to overcome all systems of exclusion. (→ #28, → #42) Even though the Internet represents a space of communicative self-actualization for many marginalized social groups (#metoo, #metwo, #schauhin, #ThingsDisabledPeopleKnow), even in digitality these groups are still particularly affected by discrimination. Digital violence, continued exclusion practices and hate speech are still present online. Sexism, racism, anti-Semitism, ableism, trans- and homophobia figure prominently in hate speech. Moreover, membership in more than one group which is targeted online increases the danger of becoming a victim of digital violence. As Amnesty International confirmed in 2018, “women of colour, religious or ethnic minority women, lesbian, bisexual, transgender or intersex (LBTI) women, women with disabilities, or non-binary individuals who do not conform to traditional gender norms of male and female, will often experience abuse that targets them in unique or compounded way“. This is dangerous. If socially discriminated groups experience additional violence in the digital sphere and therefore withdraw from participating, this effects negatively the rationality of socio-political discourse processes mediated by technology.

Discrimination in digital spaces is not limited to forms of digital violence. Rather, the Internet acts as a mirror of the society in many ways, shaping all forms of discrimination as diverse as the society itself. Technology is never neutral. Stereotypes of discrimination have been manifested in the codes and are transferred to deep learning mechanisms through the use of biased training data. The normalization and standardization of human bodies and lifestyles is implicitly inscribed in the codes. Biometric facial recognition is widely known to be unable to identify People of Colour because it usually relies solely on white training data sets. Similar to this, AI training data sets from autonomous vehicles disregard training data from non-normalized bodies such as wheelchair users.

All technologies that create, organize and expand the digital are not neutral or unbiased, but are social constructions which are always tied to existing relations of power, domination and discrimination. In doing so, they have been proven to link up with colonial practices where the collection of social data already supported the establishment of a patriarchal power structure. Digital technology by no means makes us a community of equals. Apart from some positive examples, such as empowering hashtagged movements and the possibilities to mobilize and raise awareness quickly and globally, the Internet strengthens existing systems of power and exclusion. For this reason, digital innovation must always be critically questioned.

Truth: The Internet is not a neutral platform for global empowerment. Rather information and communication technologies mirror the structures of social power and domination in our societies. They are saturated with systems of discrimination and exclusion. If left unchecked, vulnerable groups will be marginalized online as well, and prejudice and discriminatory practices will be digitalized and exacerbated.

Source

Nicole Shephard: What is sexual surveillance and why does it matter?, genderit.org (2017), https://www.genderit.org/feminist-talk/what-sexual-surveillance-and-why-does-it-matter; Rachel E. Dubrofsky, Shoshana Amielle Magnet, Feminist Surveillance Studies (Durham: Duke University Press, 2015).

MYTH #18

Das Internet fördert Emanzipation und beendet jede Form der Diskriminierung.

Nein, sagt Katharina Mosene: Das Internet ist keine neutrale Plattform für globale Förderung von Teilhabe. Vielmehr spiegeln die Informations und Kommunikationstechnologien soziale Macht und Herrschaftsstrukturen in unserer Gesellschaft wider und sind voller Diskriminierungs und Ausgrenzungssysteme. Ohne Kontrolle dieser Technologien werden gefährdete Gruppen auch online marginalisiert und Vorurteile und diskriminierende Praktiken werden digitalisiert und verschärft.

الإنترنت أداة تحرُّر لإنهاء كافة أشكال التمييز.

كلا، هكذا تقول كاترينا موسينه: الإنترنت ليست منصة محايدة للتمكين العالمي بل تعكس تكنولوجيات المعلومات والاتصال هياكل القوة الاجتماعية والهيمنة في مجتمعاتنا المشبعة بأنظمة التمييز والإقصاء. ولو تُركت بلا رقيب فسيتم تهميش الفئات الضعيفة على الإنترنت أيضًا، وسوف تُرقْمَن ممارسات التحامل والتمييز وتتفاقم.

互联网是终止所有歧视的解放工具。

不，Katharina Mosene 写道：互联网并不是全球授权的中立平台。相反，信息和通信技术反映了我们社会中社会权力和统治的结构。其中充满了歧视和排斥体制。如果不加以制止，弱势群体也将在网络上被边缘化，而且偏见和歧视性做法将增加并恶化。

Internet est un outil d‘émancipation utile pour mettre fin à toute discrimination.

Non, écrit Katharina Mosene: Internet n‘est pas une plateforme de prise de parole mondiale neutre. Les technologies de l‘information et de la communication reflètent plutôt les structures de pouvoir et de domination sociale de nos sociétés. Celles-ci sont saturées de systèmes de discrimination et d‘exclusion. Si rien n‘est fait, les groupes vulnérables seront tout autant marginalisés en ligne, et les préjugés et les pratiques discriminatoires seront numérisés et exacerbés.

Интернет – инструмент освобождения, который призван положить конец дискриминации.

Это не так, говорит Катарина Мозене: Интернет – это не нейтральная платформа для всемирного расширения прав и возможностей. Информационные и коммуникационные технологии скорее отражают структуры социальной власти и влияния в наших обществах. Они пронизаны системами дискриминации и неравноправия. Если не препятствовать этому, уязвимые группы также будут оттеснены и в Интернете, а ущемляющие и дискриминационные практики будут переведены в цифровую форму и усугублены.

El internet es una herramienta emancipadora que acabará con toda la discriminación.

No, dice Katharina Mosene: el internet no es una plataforma neutral de empoderamiento global. Las tecnologías de la información y comunicación son más bien un reflejo de las estructuras de poder social y dominación de nuestras sociedades. Están saturadas de sistemas de discriminación y exclusión. Si se dejan desatendidos, los grupos vulnerables serán marginados también en la red, y los prejuicios y las prácticas discriminatorias serán digitalizadas y se exacerbarán.

MYTH #19

Astrid Mager

Search engines provide objective results.

Myth: Search engines deliver objective search results. This is the founding myth of the leading search engine in the Western World: Google. 20 years later this founding myth still exists in Google's company philosophy. More importantly, however, it resonates in people's minds. Without knowing how the search engine actually works, many users say that the best websites can be found on top.

Busted: In 1998, the founding year of Google, Sergey Brin and Larry Page described their search engine's central aim as follows: "The primary goal is to provide high quality search results over a rapidly growing World Wide Web." (Brin and Page 1998: 115). Accordingly, the notions "quality" and "search quality" feature over 30 times in their research paper. The authors depict the PageRank algorithm – originally using the number and quality of hyperlinks a website gets, anchor text and proximity to determine the quality of a website and rank it accordingly – as their main competitive advantage. They describe the algorithm as "objective measure" corresponding well to "people's subjective idea of importance" (Brin and Page 1998: 109). Interestingly, this seems to be the case indeed. Having asked people why they use Google to find online health information in the context of my PhD project, most people answered with saying that Google delivered the best search results, implicitly shaping the search engine as a tool for quality assurance. Without knowing – or even thinking about – how the search engine actually works, Google's founding myth was reproduced in people's stories.

But it is a myth. Search engines are no neutral, objective technologies, but rather tightly intertwined with societal norms, values and ideologies; the capitalist ideology most importantly. Over the past decades, Google's "techno-fundamentalist" ideology of neutral ranking was aligned with and overshadowed by non-objective considerations. New media scholars started to deconstruct the myth of objectivity soon after the search engine's successful market entry. At first, they challenged the PageRank algorithm by arguing that it would threaten the democratic ideal of the web (→ #28) by systematically preferring big, well-connected, often commercial websites at the expense of smaller ones. Later they switched over to questioning search engines' business models based on user-targeted advertising and the commercialization of search engine results and privacy issues these trigger. A major criticism in this body of work concerns the "consumer profiling" conducted by Google – and others like Bing – that enable search engines to adjust advertisements to users' individual interests. (→ #21; → #22)

Due to the growing amount of user data these companies acquired, the search algorithm and the "organic" search results changed too. Besides hyperlinks other factors were thrown into the measuring of a website's quality including user profiles and click behaviour most particularly, but also the structure of a website, timeliness, and the amount of keywords and content. Accordingly, new media researchers, but increasingly also journalists, criticized the intensified personalization of search engine results, search engine biases and discrimination. This illustrates that search algorithms are tightly intertwined with the business models their companies rely on. The capitalist ideology is embedded in search engines and "acts through algorithmic logics and computational systems" (Mager 2014: 32).

Truth: It is important to keep in mind that search engines and their algorithms are no neutral technologies, but rather incorporate societal values and ideologies; the capitalist ideology most importantly. Only then may we come up with forward-looking governance models respecting local regulations and resonating with human rights (especially in Europe, where data protection is enshrined as a fundamental right).

Source

Sergey Brin and Lawrence Page, The anatomy of a large-scale hypertextual Web search engine, Computer Networks and ISDN Systems 30: 107–117 (1998); Astrid Mager, Defining Algorithmic Ideology: Using Ideology Critique to Scrutinize Corporate Search Engines, tripleC 12(1): 28–39 (2014).

MYTH #19

Suchmaschinen liefern objektive Ergebnisse.

Nein, sagt Astrid Mager: Man muss sich vor Augen führen, dass Suchmaschinen und ihre Algorithmen keine neutralen Technologien sind, sondern vielmehr gesellschaftliche Werte und Ideologien verinnerlichen –insbesondere solche des Kapitalismus. Nur dann können wir zeitgemäße Governance-Modelle entwickeln, die Menschenrechte respektieren (insbesondere in Europa, wo der Datenschutz als Menschenrecht verankert ist).

محركات البحث تعطي نتائج موضوعية.

كلا، هكذا تقول أستريد ماغر: من المهم أن تضع في اعتبارك أن محركات البحث وخوارزمياتها ليست تكنولوجيات محايدة، بل إنها تُضَمِّن القيم والأيديولوجيات المجتمعية وعلى رأسها الأيديولوجية الرأسمالية. وعندئذ فقط يمكن أن نتوصل إلى نماذج إدارة تطلّعية تحترم اللوائح التنظيمية المحلية وتتوافق مع حقوق الإنسان (خاصة في أوروبا التي تكرس حماية البيانات كحق أساسي).

搜索引擎提供客观结果。

不，Astrid Mager 写道：务必记住，搜索引擎及其算法并非中立技术，而是社会价值观和意识形态的结合体，其中资本主义意识形态最为重要。只有这样，我们才能提出尊重地方法规并与人权产生共鸣的前瞻性治理模式（特别是在欧洲，数据保护被视为一项基本权利）。

Les moteurs de recherche fournissent des résultats objectifs.

Non, écrit Astrid Mager: il est important de garder à l‘esprit que les moteurs de recherche et leurs algorithmes ne sont pas des technologies neutres, ils intègrent au contraire les valeurs et les idéologies de la société, notamment l‘idéologie capitaliste. Ce n‘est que si nous avons conscience de cela que nous pourrons proposer des modèles de gouvernance tournés vers l‘avenir, respectant les réglementations locales et les droits de l‘homme (en particulier en Europe, où la protection des données est inscrite en tant que droit fondamental).

Поисковые системы предоставляют объективные результаты.

Это не так, говорит Астрид Магер: Важно помнить, что поисковые системы и их алгоритмы не являются нейтральными технологиями, а скорее учитывают социальные ценности и идеологию, преимущественно капиталистическую. Только в этом случае мы сможем разработать прогрессивные модели управления, которые будут соответствовать местным законам и перекликаться с правами человека (особенно в Европе, где защита данных закреплена как фундаментальное право).

Los motores de búsqueda proporcionan resultados objetivos.

No, dice Astrid Mager: es importante tener en cuenta que los motores de búsqueda y sus algoritmos no son tecnologías neutrales, sino que más bien incorporan valores sociales e ideologías; la ideología capitalista principalmente. Solo entonces podremos concebir modelos de gobernanza con miras al futuro y que respeten las regulaciones locales y los derechos humanos (especialmente en Europa, en donde la protección de datos ha sido consagrada como un derecho fundamental).

MYTH #20

Jozef Michal Mintal

Social media is an accurate mirror of society.

Myth: Social media adequately reflects societal trends and public opinion. As everyone is on social media these days, one can determine the overall attitudes of a population by looking at what people are posting and sharing online.

Busted: There are at least two fundamentally wrong assumptions with regard to this myth. First, the notion that everyone is nowadays on social media. Even though Internet penetration and social media use saw a steep increase in the last decade, there are still vast differences in Internet and social media penetration around the world, with Internet penetration in some countries being as low as 10%. But social media users are not representative in countries with high Internet usage either. Gender, income, age and other disparities matter (Blank/Lutz 2017). Minorities, including linguistic minorities, also tend to be underrepresented on social media.

But there are also other factors which even further make it simply not possible to deduce the overall attitudes of a population just from posts and likes. (→#24)

For one, when using social media, we have a tendency to be drawn to those we perceive to be most like ourselves. (→ #21, → #22) This translates to us being exposed on average mainly to beliefs and attitudes like ours, which is a very bad base for assuming what most of the people think and like. Further, user activity on multiple social media platforms seems to follow an approximate power law distribution. (→ #41)

This means that a small number of users generate a large part of the overall content. For instance, a recent Twitter study suggests that 10% of users in the U.S. are responsible for 80% of social media content (Wojcik/Hughes 2019). The opinions of a few highly active users therefore seem far more prevalent than they are in reality.

There are also many more principles at play, like the majority illusion paradox, algorithmic bias, the creation of fake social media persona(e), etc. We should therefore be very critical of what we see online and recall that when looking at social media we cannot assume that it is an accurate mirror of society.

Truth: Social media depicts a very skewed image of society as a whole. Even though social media use is rising, social media platforms are still far from being representative of the general population. Together with factors like highly active media users, algorithmic bias and the tendency to be drawn to like-minded people and posts one agrees with, we cannot accurately determine the overall attitudes of a population just by looking at what people are posting and sharing online.

Source

Grant Blank and Christoph Lutz, Representativeness of Social Media in Great Britain: Investigating Facebook, LinkedIn, Twitter, Pinterest, Google+, and Instagram, American Behavioral Scientist 61 (2017) 7, 741–756; Stefan Wojcik and Adam Hughes, Sizing Up Twitter Users, Pew Research Center (2019), https://www.pewInternet.org/2019/04/24/sizing-up-twitter-users.

MYTH #20

Soziale Medien sind ein exakter Spiegel der Gesellschaft.

Nein, sagt Jozef Michal Mintal: Soziale Medien zeichnen ein stark verzerrtes Bild der Gesellschaft als Ganzes. Auch wenn die Nutzung sozialer Medien zunimmt, sind Social-Media-Plattformen noch lange nicht repräsentativ für die Bevölkerung. Zusammen mit Faktoren wie hochaktiven Mediennutzer*innen, algorithmischer Verzerrung und der Tendenz, sich Gleichgesinnten anzuschließen und Beiträge zu lesen, denen man zustimmt, lässt sich die allgemeine Einstellung einer Bevölkerung nicht präzise dadurch ermitteln, dass man sich anschaut, was online veröffentlicht und geteilt wird.

وسائل التواصل الاجتماعي مرآة دقيقة للمجتمع.

كلا، هكذا يقول جوزيف ميشال مينتال: تقدم وسائل التواصل الاجتماعي صورة محرَّفة للغاية للمجتمع ككل. فعلى الرغم من أن استخدام وسائل التواصل الاجتماعي في تزايد ما زالت منصات وسائل التواصل الاجتماعي بعيدة كل البعد عن كونها صورة تمثل أغلبية الناس. وبجانب عوامل أخرى كمستخدمي الوسائط بالغي النشاط والانحياز الخوارزمي وميل الشخص إلى الانجذاب نحو ذوي الفكر المتشابه معه والمنشورات التي يتفق معها، لا يمكننا أن نحدد بدقة المواقف العامة لفئة سكانية استنادًا إلى ما ينشره الأشخاص ويتشاركونه على الإنترنت فحسب.

社交媒体是社会的准确镜像。

不，Jozef Michal Mintal 写道：社交媒体描绘的是非常扭曲的社会整体形象。尽管越来越多人使用社交媒体，但社交媒体平台仍远未代表一般人群。加上高度活跃的媒体用户、算法偏见、吸引志趣相投人士的倾向以及某人同意的帖子等因素，我们无法通过查看人们在网络上发布和分享的内容准确地确定人们的整体态度。

Les réseaux sociaux sont des miroirs fidèles de la société.

Non, écrit Jozef Michal Mintal: les réseaux sociaux dépeignent une image très biaisée de la société dans son ensemble. Même si l‘utilisation des réseaux sociaux augmente, ces plateformes sont encore loin d‘être représentatives de la population en général. Avec des facteurs tels que les utilisateurs très actifs de ces réseaux, les biais algorithmiques et la tendance à attirer des personnes partageant les mêmes idées et les mêmes avis, nous ne pouvons pas déterminer avec précision le comportement général d‘une population en nous contentant de regarder ce que les gens publient et partagent en ligne.

Социальные сети безошибочно отображают общество.

Это не так, говорит Йозеф Михал Минтал: Социальные сети в целом изображают очень искаженный образ общества. Несмотря на то, что использование социальных сетей растет, их платформы все еще далеки от того, чтобы представлять население в целом. Учитывая такие факторы, как высокоактивные пользователи сетей, алгоритмическая предвзятость и склонность притягиваться к единомышленникам и постам, которые нам по душе, нельзя точно определить общее отношение населения, просто взглянув на то, что люди публикуют и чем они обмениваются в Интернете.

Las redes sociales son un reflejo fidedigno de la sociedad.

No, dice Jozef Michal Mintal: las redes sociales presentan una imagen muy sesgada de la sociedad como conjunto. Aunque el uso de las redes sociales va en aumento, estas plataformas aún están lejos de ser representativas de la población en general. Unido a factores tales como usuarios de medios muy activos, sesgos algorítmicos y la tendencia a sentirse atraído hacia personas con ideas semejantes y publicaciones con cuyo contenido se concuerda, no podemos determinar con exactitud las actitudes generales de una población solamente viendo lo que la gente está publicando y compartiendo en el internet.

MYTH #21

David Schulze

All Internet users experience the same Internet.

Myth: The Internet is the same for everyone. Some governments might block foreign content within their countries, and some content is removed to protect copyright. But all in all, if we stay in a country with free Internet or surf on accessible websites, we are all equal citizens of the Internet and treated as such.

Busted: Most users have accepted that content they watch on YouTube, search for on Google, (→ #19) or get suggested on Amazon is personalized. (→ #22) Less tolerated and frequently reviled are targeted online advertisements that show up mostly on websites using Google Ads and Facebook. But governments and companies have developed capacities, such as redirecting traffic, filters and algorithms that can have a profound yet hard to discern impact on the way we experience the Internet.

Take for example what is known as the Great Firewall, the Chinese government's program to control the Internet. While it does simply block certain foreign websites like those of The Economist and Le Monde, studies such as by The Citizen Lab at the University of Toronto have revealed a complex structure that can also slow down and redirect access requests to websites in China and abroad, and use it for offensive purposes in DDoS attacks. Censorship usually results in frustration and protest, but it can also subconsciously alter behaviour. Critical debate is obviously stifled under heavy censorship. But if some pages just happen to load very slowly, we may avoid them, without attributing it to censorship. If our request is instead rerouted, or turned into part of a DDoS attack, we might never find out.

Another example: Companies use hardware and software to modify users' experiences for commercial or even political reasons. Algorithms that may amplify familiar stories in our social media or search results are also part of other websites, e.g. Google Scholar. Internet service providers like Comcast (USA) and Bell Canada have been accused of illegally throttling certain Internet traffic, based on deep packet inspection that allows them to distinguish between data flows to their own services and those of their competitors and adjust access speed accordingly. (→ #39) Manufacturers of smartphones control how customers use apps – and through them the Internet – by making some of them harder to access or even incompatible with their operating systems. Companies also become complicit in censorship when they preemptively block user generated content perceived as illegal, or block access to their own employees' protests over work conditions.

We already live in a fragmented Internet, with breaks occurring right through countries, users' devices and websites, not just between them. The first step towards defragmentation is increasing awareness.

Truth: Internet service providers, governments, cloud, hardware and software companies have created walls, walled gardens, divides and bubbles that can profoundly shape our online experience, the way we interact with other users and how we learn about the world. These barriers are flexible, evolving and often hidden. They make us experience different parts of the Internet; and the same parts differently. Only awareness of barriers can help us overcome the fragmentation of our digital lives.

Source
Roya Ensafi, Philipp Winter, Abdullah Mueen, Jedidiah R. Crandall, Analyzing the Great Firewall of China Over Space and Time, Proceedings on Privacy Enhancing Technologies, 1 (2015), 61–76, doi: https://doi.org/10.1515/popets-2015-0005; Greg Goth, ISP Traffic Management: Will Innovation or Regulation Ensure Fairness?, IEEE Distributed Systems Online, 9 (2008) 9, https://ieeexplore.ieee.org/abstract/document/4659261.

MYTH #21

Alle Internetnutzer*innen können dasselbe Internet erleben.

Nein, sagt David Schulze: Internetdienstanbieter, Regierungen sowie Cloud, Hard und Softwareunternehmen haben Mauern, „Walled Gardens“, Trennwände und Blasen geschaffen, die unsere Onlineerfahrung, die Art und Weise, wie wir mit anderen Nutzer*innen interagieren und wie wir uns über die Welt informieren, nachhaltig prägen können. Diese Barrieren sind teils flexibel, entwickeln sich weiter und sind oftmals verborgen. Sie lassen uns verschiedene Teile des Internets erleben – und dieselben Teile anders. Nur das Wissen um die Barrieren kann uns helfen, die Fragmentierung unseres Lebens in der digitalen Welt zu überwinden.

جميع مستخدمي الإنترنت يعايشون نفس تجربة الإنترنت.

كلا، هكذا يقول دافيد شولتسه: قام مزودو خدمات الإنترنت والحكومات والخدمات السحابية وشركات الأجهزة والبرامج بإنشاء جدران وحدائق مسيَّجة وخطوط تقسيم وفقاعات يمكنها أن تشكّل وبعمق تجربتنا الإنترنتية وطريقة تفاعلنا مع المستخدمين الآخرين وكيفية تعرفّنا على العالم. وهذه الحواجز مرنة وآخذة في التطور وغالبًا ما تكون خفية، وتجعلنا نعايش أجزاء مختلفة من الإنترنت، ونعايش الأجزاء نفسها بشكل مختلف. والوعي بهذه الحواجز هو وحده الذي يمكنه مساعدتنا على التغلب على تجزُّؤ حيواتنا الرقمية.

所有互联网用户都可以有相同的互联网体验。

不，David Schulze 写道：互联网服务供应商、政府、云端、硬件和软件公司已经创建了围墙、围墙花园、分界和泡沫，可深刻地塑造我们的网络体验、我们与其他用户的互动方式以及我们了解世界的方式。这些障碍是灵活的、不断演变的且往往具有隐蔽性。它们让我们对互联网的不同和相同部分有了不一样的体验。只有意识到这些障碍，才能帮助我们克服数字化生活的碎片化。

Tous les utilisateurs d‘Internet peuvent utiliser le même Internet.

Non, écrit David Schulze: les fournisseurs de services Internet, les gouvernements, le cloud, les sociétés de matériel informatique et les éditeurs de logiciels ont créé des murs, des jardins fermés, des cloisons et des bulles qui peuvent profondément façonner notre expérience en ligne, notre façon d’interagir avec les autres utilisateurs et notre façon d’apprendre à connaître le monde. Ces barrières sont flexibles, évolutives et souvent cachées. Elles nous font découvrir différentes parties d’Internet, et les mêmes parties différemment. Seule la prise de conscience de ces barrières peut nous aider à ne pas laisser nos vies numériques se fragmenter.

Все интернет-пользователи сталкиваются с одинаковым Интернетом.

Это не так, говорит Дэвид Шульце: Интернет-провайдеры, правительства, облачные хранилища, компании, выпускающие аппаратное и программное обеспечение создали границы, закрытые экосистемы, барьеры и зоны, которые могут существенно влиять на нашу жизнь онлайн, способ взаимодействия с другими пользователями и познания мира. Эти барьеры достаточно гибкие, прогрессирующие и часто скрытые. Благодаря им мы сталкиваемся с различными частями Интернета и видим те же части по-разному. Только осознав существование этих барьеров, мы можем ослабить фрагментацию нашей цифровой жизни.

Todos los usuarios del internet experimentan el mismo internet.

No, dice David Schulze: los proveedores de servicios de internet, los gobiernos, las empresas de cloud, hardware y software han construido muros, jardines amurallados, divisiones y burbujas que pueden condicionar profundamente nuestra experiencia online, la manera en la que interactuamos con otros usuarios y nuestra visión del mundo en general. Estas barreras son flexibles, cambiantes y se encuentran frecuentemente ocultas. Se nos hace experimentar diferentes lugares del internet; y los mismos lugares de forma distinta. Solamente la conciencia respecto a estas barreras puede ayudarnos a superar una posible fragmentación de nuestras vidas digitales.

MYTH #22

Sebastian Randerath

We all live in filter bubbles.

Myth: Filter bubbles run our whole life. Political, social and economic problems like the rise of populism, hate speech, fake news, growing capitalism and even depressions are caused by the personalization of search engines and social media platforms as well as by micro targeting. Filter bubbles and echo chambers separate users from each other by creating invisible bubbles.

Busted: Conceptually, filter bubbles exist. (→ #21) In 2009, Google included algorithms in its search tools that were personalized by individual user data. In 2011, Eli Pariser claimed that this meant that no “standard” (common) Google search outcome existed. This is what he called a “filter bubble” – a space inside search algorithms and social media platforms that uses data to personalize a specific “bubble” for every single user. Today, in view of the rise of large platforms like Facebook, Google, Alibaba and Baidu models of data accumulation and micro-targeting are part of a new data-driven capitalism (Srnicek 2016).

Today, Pariser’s filter bubble is used to explain different social, economic and digital phenomena like the growth of populism, hate speech, fake news, growing capitalism and even depression. Often the concept of the echo chamber that existed long before the filter bubble and had been already employed by Marshall McLuhan to describe the resonating world of tribal cultures (McLuhan/Norden 1969: 72) is misused to extend the concept of being (consciously or automatically) separated from dissenting world views on social media platforms. Filter bubbles and echo chambers have become blurry concepts to simplify different and complex phenomena of decision-making and formation of public opinion.

As numerous studies on public opinion formation have shown, network effects (→ #41) and other communicative structures that are caused by relations in social media have a much stronger impact on the formation of public opinion on platforms than algorithmic filtering (Haim et al., 2018). Empirically there has even been no direct proof that there is an effect of personal filtering on networks and formations of public opinion (Krafft et al. 2018) and even the direct effects of the algorithms on the personalization itself are very trivial (Feuz/Fuller/Stalder 2011). Political segmentations in populist debates on social media are mainly caused by the dynamics of populism itself, network effects or social bots and not directly by filtering algorithms (Dreyer/Schulz, 2019; Leistert 2017). Filter bubbles in search algorithms are not the ultimate cause for network effects, hate speech, populism or fake news – they have just become a metaphor to simplify these complex processes.

Truth: Filter bubbles do not run our lives. Personalized filtering by algorithms is not the cause for public opinion formation and has merely trivial effects on search results with major search engines. The concept is mainly used as a metaphor to reduce the complexity of social, economic and technological dynamics on platforms and public debates, but is of little value beyond that.

Source

Mario Haim, Andreas Graefe, Hans-Bernd Brosius, Burst of the filter bubble? Effects of personalization on the diversity of Google News, Digital Journalism (2018) 6 (3), 330–343; Martin Feuz, Matthew Fuller and Felix Stalder, Personal Web Searching in the Age of Semantic Capitalism: Diagnosing the Mechanisms of Personalisation, First Monday (2011) 16 (2), doi:10.5210/fm.v16i2.3344.

MYTH #22

Wir leben alle in Filterblasen.

Nein, sagt Sebastian Randerath: Filterblasen bestimmen unser Leben nicht. Die personalisierte Filterung durch Algorithmen beeinflusst nicht maßgeblich öffentliche Meinungsbildungsprozesse und hat lediglich vernachlässigbare Auswirkungen auf die Suchergebnisse großer Suchmaschinen. Das Konzept wird hauptsächlich als Metapher verwendet, um die Komplexität der sozialen, wirtschaftlichen und technologischen Dynamik auf Plattformen und in der öffentlichen Diskussion zu reduzieren, ist aber darüber hinaus von geringem Wert.

جميعنا يعيش في فقاعة تصفية.

كلا، هكذا يقول سيباستيان رانديرات: فقاعات التصفية لا تُدير حياتنا. التصفية ذات الطابع الشخصي حسب الخوارزميات ليست السبب في تكوين الرأي العام وتأثيراتها على نتائج البحث باستخدام محركات البحث الرئيسية تكاد لا تُذكر. ويُستخدم هذا المفهوم بشكل أساسي كتعبير مجازي للحد من تعقيد الديناميات الاجتماعية والاقتصادية والتكنولوجية على المنصات والنقاشات العامة، لكن قيمته ضئيلة فيما عدا ذلك.

我们都生活在过滤气泡中。

不，Sebastian Randerath 写道：过滤气泡不会主导我们的生活。算法的个性化过滤不是舆论形成的原因，且仅对使用主要搜索引擎搜索的结果产生微不足道的影响。这个概念主要用作隐喻，以减少平台和公开辩论的社会、经济和技术动态的复杂性，但除此之外没什么价值。

Nous vivons tous dans des bulles de filtres.

Non, écrit Sebastian Randerath: les bulles de filtre ne conditionnent pas nos vies. Le filtrage personnalisé par algorithmes n’est pas la cause de la formation de l’opinion publique et n’a que des effets moindres sur les résultats de recherche des principaux moteurs de recherche. Le concept est principalement utilisé comme une métaphore pour réduire la complexité de la dynamique sociale, économique et technologique sur les plateformes et dans les débats publics, mais a peu de valeur en-deçà.

Мы все живем внутри пузырей-фильтров.

Это не так, говорит Себастьян Рандерат: Пузыри-фильтры не управляют нашей жизнью. Персонализированная фильтрация по алгоритмам не является причиной формирования общественного мнения и оказывает лишь ограниченное воздействие на результаты поиска в основных поисковых системах. Эта концепция в основном используется в качестве метафоры, чтобы уменьшить сложность социальной, экономической и технологической динамики на платформах и для общественного обсуждения, и малоценна помимо этого.

Todos vivimos en filtros burbuja.

No, dice Sebastian Randerath: los filtros burbuja no controlan nuestras vidas. El filtrado personalizado por algoritmos no es la causa de la formación de la opinión pública y tiene solo efectos triviales en los resultados de los motores de búsqueda más importantes. El concepto se utiliza sobre todo como metáfora para reducir la complejidad de las dinámicas sociales, económicas y tecnológicas de las plataformas y debates públicos, pero tiene muy poco valor al margen de eso.

MYTH #23

Sascha Hölig

People get their news only via social media.

Myth: People, and especially young Internet users, get their news only via social media. They ignore traditional news media. We live in filter bubbles, fall for fake news and are manipulated in our decision-making by social media content.

Busted: It is true that many people use social media. For example, 74 percent of adult Internet users in the US use Facebook, Twitter or Instagram within a regular week; in Germany this figure is 58 percent (Reuters Institute Digital News Study 2019). It is also true that some people, accidentally or not, encounter news content on social media. Be it because they see forwarded articles, because they learn about discussions on current topics, because they receive advertisements from news outlets or because they follow news media, journalists or politicians.

Overall, however, people mainly use traditional news media brands for their information, either via the corresponding websites or apps on the Internet (US: 43%; Germany: 47 %), or via real, actual television, radio, newspapers and magazines (US: 69 %; Germany: 83 %), which continue to play an important role, too. In our news consumption, as in anything else, we, humans, are intricate creatures. People obtain information through an individually compiled combination of different news outlets, the so-called "news repertoire", which often is based on cross-media use.

For some people, social media is definitely a part of their news repertoire (US: 46 %; Germany: 34 %), but just for a few users it is the most important news source (US: 18 %; Germany: 10 %) and only for a small minority of people who are not at all interested in hard news it is the only one used news source (US: 5,6 %; Germany: 2,7 %). In this pattern, there are hardly any differences between older and younger age groups. Although older users are a little more interested in news about the world than younger ones, young users nevertheless inform themselves via various news sources and mainly pursue their age-dependent interests in social media.

In studies after studies, it holds true that social media are mainly used to get and exchange information about the latest developments from the circle of friends and acquaintances, but not to consume general news, nor to search for them explicitly. Social media are not perceived as a suitable place for news and the wide diversity of actors who spread news there is little trusted. Therefore, for most people across the age groups, news information in social media is merely a by-catch that cannot be avoided.

Users who actively choose to follow news content in social media are in a minority compared to the total number of users. Those who follow news sites, journalists and politicians are usually those who are particularly interested in current news topics and they use a particularly broad and diverse news repertoire of numerous news outlets, likewise outside of social media.

Therefore, it is true that some people encounter news in social media, but usually this is not an intended source for news information, nor is it their only source for news. The assumption that even young people only get news via social media is just a persistent myth.

Truth: Social media plays an important role in many people‘s lives but social media are usually not used for the purpose of getting news information. News is rather a kind of inevitable by-catch for social media users. The vast majority of Internet users across all age groups uses traditional news media brands on- and offline, and only a small minority of social media users limits its news consumption to social media platforms.

Source

Uwe Hasebrink and Sascha Hölig, Deconstructing Audiences in Converging Media Environments, in Sergio Sparviero, Corinna Peil, Gabriele Balbi (eds.), Media Convergence and Deconvergence (Basingstoke: Palgrave Macmillan, 2017), 113-133. doi: 10.1007/978-3-319-51289-1_6; Nic Newman, Richard Fletcher, Antoins Kalogeropoulos, Rasmus Kleis Nielsen, Reuters Institute Digital News Report 2019 (University of Oxford: Reuters Institute for the Study of Journalism, 2018), www.digitalnewsreport.org.

MYTH #23

Die Menschen informieren sich nur noch über soziale Medien.

Nein, sagt Sascha Hölig: Auch wenn soziale Medien im Leben vieler Menschen eine wichtige Rolle einnehmen, werden sie in der Regel nicht zum Zweck der Informationsbeschaffung genutzt. Nachrichten sind eher eine Art unvermeidlicher Nebennutzen für aktive Nutzer*innen sozialer Medien. Die überwiegende Mehrheit der Internetnutzer*innen aller Altersgruppen verwendet traditionelle Nachrichtenkanäle on und offline, und nur eine kleine Minderheit der Nutzer*innen von sozialen Medien beschränkt ihren Nachrichtenkonsum ausschließlich auf diese Plattformen.

لا يحصل الناس على الأخبار إلا عبر وسائل التواصل الاجتماعي.

كلا، هكذا يقول ساشا هوليغ: تلعب وسائل التواصل الاجتماعي دورًا هامًا في حياة الكثير من الناس، لكن لا تُستخدم وسائل التواصل الاجتماعي عادةً بغرض الحصول على معلومات إخبارية. والأخبار بالأحرى أشبه بثمرة ثانوية حتمية يجنيها مستخدمو وسائل التواصل الاجتماعي. فالغالبية العظمى من مستخدمي الإنترنت عبر كافة الفئات العمرية يستخدمون الوسائط الإخبارية التقليدية على الإنترنت وخارجها، وليست هناك إلا قلة قليلة من مستخدمي وسائل التواصل الاجتماعي تقتصر على منصات الوسائط الاجتماعية في استقائها الأخبار.

人们只能通过社交媒体获取新闻。

不，Sascha Hölig 写道：社交媒体在很多人的生活中发挥着重要作用，但社交媒体通常不用于获取新闻信息。对于社交媒体用户而言，新闻只是一种无法避免的间接渔获。所有年龄段的绝大多数互联网用户都在线上和线下使用传统新闻媒体品牌，只有少数社交媒体用户将其新闻消费限制在社交媒体平台上。

Les personnes ne s‘informent que via les réseaux sociaux.

Non, écrit Sascha Hölig : si les réseaux sociaux jouent un rôle important dans la vie de nombreuses personnes, ils ne sont généralement pas utilisés pour s‘informer. Les informations ou actualités sont plutôt une sorte de prise accessoire inévitable pour les utilisateurs des réseaux sociaux. La grande majorité des utilisateurs d’Internet de tous les groupes d’âge utilisent des moyens d’information classiques en ligne et hors-ligne, et seule une petite minorité d’utilisateurs des réseaux sociaux limite sa recherche d’informations à ces plateformes.

Люди узнают новости только через социальные сети.

Это не так, говорит Саша Хёлиг: Социальные сети играют очень важную роль в жизни многих людей, но как правило не используются в целях получения новостей. Новости – это скорее неизбежный прилов для пользователей социальных сетей. Подавляющее большинство интернет-пользователей всех возрастных групп используют традиционные новостные СМИ как онлайн, так и офлайн, и лишь небольшая часть пользователей ограничивает свое знакомство с новостями платформами социальных сетей.

Las personas obtienen las noticias solo por medio de las redes sociales.

No, dice Sascha Hölig: las redes sociales juegan un papel importante en la vida de muchas personas, pero no son usadas normalmente con el fin de obtener información relativa a noticias. Las noticias en este contexto representan más bien información secundaria adquirida por los usuarios de redes sociales. La gran mayoría de usuarios del internet, en todos los grupos de edad, consulta los medios tradicionales de noticias, tanto online como offline, y solo un pequeña minoría de los usuarios limita su consumo de noticias a las plataformas de redes sociales.

MYTH #24

Ulrike Klinger

Likes and shares reliably indicate popularity.

Myth: Likes, shares, views, follower numbers and other quantitative measures on social media reliably indicate how popular, famous, or successful someone or something is. A growth of likes or followers always means a positive feedback and we can rely on them as trend indicators.

Busted: The perception that likes, shares, or the number of one´s followers and "friends" on social media indicate popularity is widespread. Marketing suggests they are a shortcut to measure how well a brand or a person is doing. Parents and educators worry about teenagers' obsession with how many hearts they get on Instagram. In election campaigns, journalists discuss political parties and candidates' success in mobilizing by comparing followers and reactions. The idea that quantifiable social cues are an easy way to evaluate popularity is compelling. Unfortunately, it is also a misunderstanding, because a) they are very easy to manipulate and b) they mean different things depending on context and platform.

The idea of likes, shares and a large number of followers as popularity cues has incentivized people and organizations to artificially enhance these numbers. With the help of automated accounts ("social bots"), trolls, activists, and fake accounts it is very easy to feign popularity cues and make something or someone seem more "popular". (→ #30) In fact, social media platforms report that they are deleting billions of these fake or maliciously manipulative accounts each year. Everyone can easily and for very little money buy likes, shares or followers; it is a common practice and turns these popularity cues in empty signifiers. In political mobilization this phenomenon has been labelled "astroturfing" – feigning popular support and grassroots mobilization with artificial activity and fake accounts.

Likes and shares are ubiquitous on social media. We all like or share something several times a day and hope that our postings get likes and shares from our imagined audiences. Turns out that people care more about who likes and shares rather than how many times: most important are close friends, spouses and family. Likes signal acknowledgement, but not always agreement or acceptance. As for political parties, social media users tend to follow not only one, but several parties, and cross-posting on more than one political group is quite a usual behaviour. People oftentimes share content without even reading it before sharing (clickbait!), and they share and comment postings they heavily disagree with. In fact, controversial content often generates high levels of engagement – many likes, shares and comments, but certainly not because of popularity or agreement.

Truth: The numbers of likes, shares, followers or comments provide low-level feedback, signalling acknowledgement, reach, engagement or interaction. This feedback is not necessarily and always positive. It can mean popularity, but it might as well indicate that something or someone is even unpopular or highly controversial. These numbers are easy to manipulate and should not be overestimated.

Source

Lauren Scissors, Moira Burke, Stephen Wengrovitz, What's in a Like?: Attitudes and behaviors around receiving Likes on Facebook. CSCW ,16 Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (2016), https://dl.acm.org/citation.cfm?id=2820066; Pablo Porten-Cheé, Jörg Haßler, Pablo Jost, Christiane Eilders, Marcus Maurer, Popularity cues in online media: Theoretical and methodological perspectives. Studies in Communication and Media 7 (2018) 2, 208–230.

MYTH #24

Likes und Shares sind ein zuverlässiges Maß für Beliebtheit.

Nein, sagt Ulrike Klinger: Die Zahl der Likes, Shares, Follower oder Kommentare ist nur sehr eingeschränkt aussagekräftig im Sinne einer Signalisierung von Zustimmung, Reichweite, Engagement oder Interaktion. Dieses Feedback ist nicht unbedingt und immer positiv. Es kann Beliebtheit bedeuten, könnte aber auch darauf hinweisen, dass etwas oder jemand sogar unbeliebt oder höchst umstritten ist. Diese Zahlen sind leicht zu manipulieren und sollten nicht überbewertet werden.

الإعجابات والمشاركات تدل بشكل موثوق على الشعبية.

كلا، هكذا تقول أولريكه كلينغر: توفر أرقام الإعجابات أو المشاركات أو المتابعين أو التعليقات ملاحظات تقييمية منخفضة المستوى، حيث تدل على الإفادة بالعلم أو الوصول أو الانخراط أو التفاعل. وهذه الملاحظات التقييمية ليست بالضرورة دائمًا إيجابية. وفي حين أنها يمكن أن تدل على الشعبية، لكنها يمكن أن تدل وبالقدر نفسه على أن الشيء أو الشخص عديم الشعبية أو مثير للجدل إلى حد كبير. يسهل التلاعب بهذه الأرقام، وينبغي ألا نبالغ في تقديرها.

喜欢和分享确切地表明受欢迎程度。

不，Ulrike Klinger 写道：喜欢、分享、关注或评论的数量提供低级反馈、信号确认、覆盖面、参与或互动。这种反馈不一定总是积极的。它可能意味着受欢迎，但也可能表明某事或某人不受欢迎或极具争议性。这些数字易于被操纵，不应高估。

Les « j‘aime » et les partages sont des indications fiables de popularité.

Non, écrit Ulrike Klinger: le nombre de « j‘aime » (like), de partages, d‘abonnés ou de commentaires fournit des informations de faible qualité et n‘est pas l‘expression d‘une réelle reconnaissance, d‘une voix majoritaire, d‘une implication ou d‘une volonté d‘interaction. Ces retours ne sont pas nécessairement et toujours positifs. Cela peut être un signe de popularité, mais cela peut tout aussi bien indiquer que quelque chose ou quelqu‘un est impopulaire ou très controversé. Ces chiffres sont faciles à manipuler et ne doivent pas être surestimés.

Лайки и репосты объективно отображают популярность.

Это не так, говорит Ульрике Клингер: Число лайков, репостов, подписчиков или комментариев плохо сигнализирует об обратной связи, признании, охвате, вовлеченности и взаимодействии. Такая обратная связь необязательна и неизменно позитивная. Она может означать популярность, но также может указывать на то, что кто-то или что-то не имеет популярности или крайне противоречиво. Этими цифрами можно с легкостью манипулировать, поэтому их значение не следует переоценивать.

Los likes y shares son un indicador de popularidad fiable.

No, dice Ulrike Klinger: el número de likes, shares, seguidores o comentarios representa una forma de feedback de nivel bajo, señalando reconocimiento de la información, alcance, participación o interacción. Este feedback no siempre es necesariamente positivo. Puede significar popularidad, pero también podría significar que algo o alguien es incluso impopular o altamente controvertido. Estos números son fáciles de manipular y no deberían ser sobreestimados.

MYTH #25

Tommaso Venturini

Fake news is a real problem.

Myth: Digital media have become, in the last few years, a space for the circulation of all sorts of false information. Ill-intentioned social and political actors have strategically used disinformation campaigns, disguised as mainstream news, to promote untruthful or incorrect ideas distorting public debates by made-up evidence.

Busted: As digital media and online spaces become crucial arenas for public debate, online misinformation is becoming a serious societal concern. Yet, the notion of “fake news” is a very bad label for this phenomenon and misleads our societal responses rather than guiding them. By now everything can be called “fake news” and the term is routinely used by politicians to identify reporting they disagree with. We should thus be wary of this notion: Fake news is an extremely vague term that has been used to refer to phenomena as diverse as real news, satire, parody, fabrication, manipulation, click-bait, conspiracy theories and covertly sponsored contents. In the absence of a strict definition, the notion lends itself to be used by political and social actors as a rhetoric weapon to discredit opposing sources of information. Also, while fake news is supposed to be a recent problem, connected to the advent of digital media, its vague connotation of “biased information influencing public debate” makes it indistinguishable from traditional propaganda.

Heralding a “post-truth era”, the notion presupposes a simplistic distinction between true and false, denying the very essence of journalistic mediation whose value is not only measured by the correspondence to the reported facts, but by the capacity to make complex issues readable for a distracted public opinion. Finally, and most importantly, the label implies that “fake news” resemble traditional news and that their main objective is to induce credulity. This is sometimes but not always the case: much misinformation is published in satirical pages that do not hide their untruthfulness; or by news outlets that play out front their ideological biases; and often is nothing but a catchy title used to lure readers into clicking on banners or opening pages.

While some online misinformation is indeed meant to trick its readers into believing it (such as strategic disinformation campaigns), this is rarely the only or its main purpose. Rather than its fakeness, the speed with which it spread and the distraction that it produces are the birthmark of this type of information that should rather be called “junk news.” Just as junk food, digital misinformation is consumed because it is addictive, not because it is believed to be informative or intellectually nourishing. To be sure, shifting the attention from falsity to diffusion and distraction does not make the threat of junk content less relevant. Quite the contrary, it suggests that these contents are all the more dangerous because they cannot be defused simply by debunking them.

Truth: The notion that “fake news” is the main menace to online public debate is itself a sort of “fake news”. The threat of digital misinformation consists in the systemic degradation of public debate, produced by the acceleration of attention cycles and the inflation of information agendas. Most fake news contents are in fact “junk news”, which does not make them less dangerous, but more difficult to debunk.

Source

Henry Jenkins, Sam Ford, and Joshua Benjamin Green, Spreadable Media (New York: New York University Press, 2013); Tommaso Venturini, From Fake to Junk News, the Data Politics of Online Virality, in Didier Bigo, Engin Isin, and Evelyn Ruppert (eds.), Data Politics: Worlds, Subjects, Rights (London: Routledge, 2019).

MYTH #25

Fake News sind ein ernstes Problem.

Nein, sagt Tommaso Venturini: Die Vorstellung, dass „Fake News“ die Hauptbedrohung für die öffentliche Diskussion im Netz darstellten, ist selbst eine Art „Fake News“. Die Bedrohung durch digitale Fehlinformationen besteht im systemischen Qualitätsverlust der öffentlichen Diskussion durch immer kürzere Aufmerksamkeitsspannen und die Inflation von Informationsagenden. Die meisten Inhalte von „Fake News“ sind eigentlich „Junk News“, was sie jedoch nicht weniger gefährlich, sondern nur schwieriger zu entlarven macht.

الأخبار الزائفة مشكلة حقيقية.

كلا، هكذا يقول توماسو فنتوريني: فكرة أن «الأخبار الزائفة» تعتبر الخطر الرئيسي المحدق بنقاش الرأي العام على الإنترنت هي في حد ذاتها نوع من «الأخبار الزائفة». يكمن تهديد التضليل الرقمي في التدهور النُّظُمي للنقاش العام الناتج عن تسارع دورات الاهتمام وتضخُّم أجندات المعلومات. غالبية محتويات الأخبار الزائفة هي في الواقع «أخبار غير هامة»، وهذا لا يجعلها أقل خطورة بل يجعل كشفها أصعب.

假新闻是真正的问题。

不，Tommaso Venturini 写道：“假新闻”是网络公开辩论主要威胁的概念本身就是一种“假新闻”。数字化错误信息的威胁在于注意力循环加速和信息议程膨胀所产生的公开辩论的系统性退化。事实上，大多数假新闻内容都是“垃圾新闻”，这并不会降低它们的危险性，但更难以揭穿。

Les intox (fake news) sont un réel problème.

Non, écrit Tommaso Venturini: la notion selon laquelle les « intox » constituent la principale menace pour le débat public en ligne est en soi une sorte d’ « intox ». La menace de désinformation numérique consiste en la dégradation systémique du débat public produite par l’accélération des cycles de l’attention et l’inflation des flux d’informations. La plupart des contenus de ces fausses nouvelles sont en fait des « informations poubelles », ce qui ne les rend pas moins dangereux, mais plus difficiles à débusquer.

Ложные новости – реальная проблема.

Это не так, говорит Томмазо Вентурини: Утверждение о том, что «ложные новости» – главная угроза для общественного онлайн-обсуждения, само по себе является своего рода «ложной новостью». Угроза цифровой дезинформации заключается в системном ослаблении общественного обсуждения, вызванном ускорением циклов внимания и раздуванием информационных программ. Большинство ложного новостного контента – это на самом деле просто «мусор», что не делает его менее опасным, а скорее усложняет процесс его разоблачения.

Las fake news son un problema real.

No, dice Tommaso Venturini: la noción de que las llamadas “fake news” son la principal amenaza para el debate público online representa en sí misma una especie de “fake news”. La amenaza de la desinformación digital consiste en una degradación sistémica del debate público producido por la aceleración de los ciclos de atención y la inflación de las agendas de información. La mayoría de los contenidos de las fake news son de hecho “noticias basura”, lo cual no las hace menos peligrosas, sino más difíciles de desmentir.

MYTH #26

Michael S. Daubs

We are all journalists and news creators now.

Myth: The Internet will enable citizens to contribute user-generated content and co-create the news and avoid the gatekeeping mechanisms of traditional news organizations, thus democratizing journalism.

Busted: In the late 1990s, user-led citizen journalism sites such as Indymedia emerged that provided the opportunity for people to "become the media" by creating and sharing user-generated content (UGC) in the form of citizen journalism. Blogging and social networking sites such as Facebook, YouTube and Twitter followed, as did citizen journalism portals from news organizations such as CNN's iReport. Many credited these platforms with democratizing journalism. (→ #28) Such views echo broader claims that digital media support a "democratic urge to allow more people to create and circulate media" (Jenkins 2006).

Arguments that UGC is inherently democratizing, however, ignore the complex relationships between the users and traditional journalistic institutions. The ability to create and share information does not necessarily guarantee access to an audience. Furthermore, many citizen journalists lack the training, fact-checking, editorial review, and motives of traditional journalists. Some citizen journalists, for example, create UGC that is more in line with opinion and commentary than explicitly political in nature. While Sharon Docter (2010) notes that arguments against classifying bloggers as journalists rarely claim that "bloggers do not contribute to the public sphere, as professional journalists do", these factors have led to ongoing debates about whether citizen journalists are subject to the same special protections afforded to traditional journalists such as shield laws that exempt journalists from having to disclose confidential sources and unpublished notes.

In short, there are many reasons to question the myth that the Internet has democratized journalism. Moreover, John T. Caldwell (2004) notes that television has "proven resilient in adapting to a series of fundamental economic, technological, and cultural changes." Traditional news organizations have, for example, increasingly incorporated UGC in their reporting rather than being threatened by it. Furthermore, some citizen journalists, who aspire to be professional journalists in the future, perform a significant amount of labour in the hopes of improving their skills and future job projects. Journalistic institutions readily capitalize on this unpaid labour, sometimes referred to as "hope labour" (Kuehn and Corrigan 2013) or "aspirational labour" (Duffy 2017), which allows traditional journalistic institutions to save money, act as an authority over UGC, and maintain their "social power to frame the issues" (Andrejevic 2004).

Truth: Because traditional journalistic institutions maintain a privileged position to select and contextualize the contributions of users, Internet-distributed user-generated content in the form of citizen journalism often results in reaffirming the authority, power and centrality of these organizations and their journalists rather than democratizing journalism.

Source

Michael S. Daubs, The Social News Network: The Appropriation of Community Labour in CNN's iReport, The Political Economy of Communication, 3.2 (2015), 55-73; Sara Platon and Mark Deuze, Indymedia Journalism: A Radical Way of Making, Selecting and Sharing News?, Journalism 4.3 (2003), 336–55.

MYTH #26

Heutzutage sind wir alle Journalist*innen und Berichterstatter*innen.

Nein, sagt Michael S. Daubs: Da traditionelle journalistische Institutionen eine privilegierte Position hinsichtlich der Auswahl und Kontextualisierung der Beiträge von Nutzer*innen einnehmen, stärken im Internet veröffentlichte nutzer*innengenerierte Inhalte in Form von Graswurzeljournalismus oftmals die Autorität, Macht und Zentralität dieser Organisationen und ihrer Journalist*innen und führen keineswegs zu einer Demokratisierung des Journalismus.

كلنا الآن صحفيون وكاتبو أخبار.

كلا، هكذا يقول مايكل إس دوبز: نظرًا لأن المؤسسات الصحفية التقليدية تتبوأ مركزًا مميزًا لانتقاء مساهمات المستخدمين ووضعها في سياقها، فإن المحتوى المُنشأ من قِبل المستخدم والموزَّع على الإنترنت على هيئة صحافة المواطن غالبًا ما يعيد تأكيد سلطة هذه المؤسسات وصلاحياتها ودورها المحوري عوضاً عن إضفاء الطابع الديمقراطي على الصحافة.

我们现在都是记者和新闻创作者。

不，Michael S. Daubs 写道：由于传统的新闻机构在选择和保护用户的贡献方面享有特权，因此通过互联网以公民新闻形式分发的用户生成内容往往再次肯定了这些组织及其记者的权限、权力和中心地位，而非新闻民主化。

Nous sommes désormais tous des journalistes et des créateurs d‘informations.

Non, écrit Michael S. Daubs : les institutions journalistiques traditionnelles conservant une position privilégiée quant à la sélection et la contextualisation des contributions des utilisateurs, le contenu généré par ces derniers sur Internet sous la forme de journalisme citoyen réaffirme souvent l‘autorité, le pouvoir et le caractère central de ces organisations et de leurs journalistes plutôt que du journalisme du tout un chacun.

Все мы сейчас журналисты и создатели новостей.

Это не так, говорит Майкл С. Даубс: Поскольку традиционные журналистские учреждения имеют привилегированное положение для отбора и контекстуализации вклада пользователей, пользовательский контент, распространяемый через Интернет в форме массовой журналистики, часто подтверждает авторитет, власть и центральное положение этих организаций и их журналистов, нежели демократизирует журналистику.

Hoy en día todos somos periodistas y creadores de noticias.

No, dice Michael S. Daubs: debido a que las instituciones periodísticas tradicionales mantienen una posición privilegiada al seleccionar y contextualizar las contribuciones de los usuarios, el contenido generado por usuarios y distribuido en el internet en forma de periodismo ciudadano frecuentemente reafirma la autoridad, poder y centralismo de estas organizaciones y sus periodistas, más que democratizar el periodismo.

MYTH #27

Claudia Lampert

Millennials are all Internet-savvy “digital natives”.

Myth: Children grow up in mediatized environments, know the Internet intimately, appropriate digital media easily and thus adopt media literacy automatically. Compared to them, adults are often seen as “digital immigrants” who have no chance of using the Internet and online media as virtuously as present and future young generations.

Busted: Children are exposed to digital media increasingly earlier. Even babies and toddlers see their parents or caregivers using smartphones or mediated via screens. Devices with touch screens or voice control (e.g. digital assistants like Siri or smart speakers like Alexa) do not require any writing or keyboard skills, so that even very young children can very easily use digital applications. Current data show that the spread of digital mobile devices has increased in recent years and that the age at which children get their first own smartphones continues to decrease. For most teenagers in western countries it is now common to own a smartphone. However, the digital possibilities are used very diversely, mostly for communication and entertainment, less for information and participation. But it is the natural and (sometimes very) intensive use of the various digital possibilities which conveys the impression that children master digital technologies and handle them more competently than adults.

However, we often disregard that self-determined, sovereign media handling requires more than technical use. On the one hand, a certain understanding of media, media-related structures and functionalities is needed to assess and classify different media (e.g. What distinguishes public from commercial programs? What are algorithms and how do they impact online content and usage? How does, e.g., online advertising work? What is an influencer?). On the other hand, self-determination also means that the media are used as ways of expression, to articulate one‘s own views, without violating dignity and rights of others. Finally, it is also a matter of reflecting on the possibilities and risks of digitization on an individual and societal level and using the creative and participatory potential of different media.

Current studies show that adolescents – depending on, e.g., age, social context and educational background – use digital opportunities in very different ways and that the skills are very differently developed. It still seems that those with privileged socio-economic status and higher educational backgrounds use digital opportunities in more diverse ways and therefore benefit more from them. The differences also point to the fact that (digital) inequalities have shifted from access (“digital divide”) to use (“second digital divide”). For educational institutions, this means that not only the technical infrastructure should be considered and optimized, but especially the use and reflection of digital online programs.

Truth: The fact that children grow up in mediatized environments does not mean that all use digital media (equally) competently. On the one hand the individual requirements are very different, on the other hand a self-determined and sovereign use requires more than technical skills.

Source

Eszter Hargittai und Yuli Patrick Hsieh, Digital Inequality, in William H. Dutton (ed.), The Oxford Handbook of Internet Studies (Oxford: OUP, 2013), DOI: 10.1093/oxfordhb/9780199589074.013.0007; Marc Prensky, Digital Natives, Digital Immigrants, On the Horizon (2001), www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf.

MYTH #27

Alle Millennials sind internetaffine „Digital Natives“.

Nein, sagt Claudia Lampert: Die Tatsache, dass Kinder in einem medienbestimmten Umfeld aufwachsen, bedeutet nicht, dass auch alle Kinder die digitalen Medien auf (gleichermaßen) kompetente Weise nutzen. Einerseits sind die individuellen Anforderungen sehr unterschiedlich, und andererseits erfordert eine selbstbestimmte und souveräne Nutzung mehr als nur technische Fähigkeiten.

أبناء جيل الألفية جميعهم «مواطنون رقميون» بارعون في الإنترنت.

كلا، هكذا تقول كلاوديا لامبرت: حقيقة أن الأطفال يكبرون في بيئات مؤطَّرة وسائطيًّا لا يعني أنهم جميعًا يستخدمون الوسائط الرقمية (على قدم المساواة) بكفاءة. فمن ناحية، تختلف المتطلبات الفردية اختلافًا كبيرًا، ومن ناحية أخرى، يتطلب الاستخدام المستقل وذو السيادة أكثر من مجرد مهارات فنية.

千禧一代都是精通互联网的“数字原生代”。

不，Claudia Lampert 写道：儿童在媒体环境中成长的事实并不意味着所有人都有资格（平等地）使用数字媒体。一方面，个人要求差异很大，另一方面，自我决定和独立使用数字媒体需要的不仅仅是技术技能。

Les individus de la génération Y ont tous baigné dans le numérique et sont habitués à Internet.

Non, écrit Claudia Lampert: le fait que les enfants grandissent dans des environnements dans lesquels le numérique est très présent ne signifie pas que tous ont les compétences pour l‘utiliser (de manière identique). Les exigences individuelles sont d‘une part très différentes, et d‘autre part, une utilisation autonome et indépendante nécessite plus que des compétences techniques.

Миллениалы – разбирающееся в вопросах Интернета «цифровое поколение».

Это не так, говорит Клаудия Лампeрт: Тот факт, что дети растут в медиасреде, не означает, что все используют цифровые медиа (одинаково) грамотно. С одной стороны, индивидуальные требования очень разные, с другой, самостоятельное использование на высоком уровне требует не просто технических навыков.

Todos los millenials son expertos en el internet o digital natives.

No, dice Claudia Lampert: el hecho de que los niños crezcan en ambientes mediatizados no significa que todos usen los medios digitales de manera (uniformemente) competente. Por un lado, los requisitos individuales son muy diferentes y por el otro, un uso autodeterminado y ejemplar requiere algo más que solo habilidades técnicas.

MYTH #28

Laeed Zaghlami

The Internet promotes democracy, like during the “Arab Spring”.

Myth: Social media empowers the marginalized and the oppressed alike. Internet and social media as soft power assets exert pressures on political regimes to shift from authoritarianism to democratic and pluralistic societies. Social movements and uprisings like the Arab Spring are only made possible by the Internet and will occur wherever Internet access exceeds a certain reach.

Busted: Yes, the Internet and social media specifically played a role in spreading awareness and organizing protests in all countries where the so-called Arab Spring “revolutions” took place. However, it has been shown in several studies since then that neither Internet-savvy young liberals have been the driving force in this turmoil, nor did regime changes result in newly democratized nation states. Arab Spring seems in itself a rather controversial and ambiguous notion, as it is now turning Egypt, Libya, Sudan and Tunisia into a state of turmoil, disorder and terror after the euphoria of the first years. Moreover, the movement has not led to substantial gains in terms of democratic norms, values and practices in all nations in the region.

Take the example of Algeria as one of those countries that could have seized democratic opportunities to move to a more social justice and freedom of the press. But its citizens are still striving to freely express their opinions and implement democratic ideals. Substantial changes in Algeria have not come out as direct results of Internet and social media use; the latter were mere tools of information, interaction and communication. Rather, calls for political pluralism, social justice and press freedom are deeply rooted in the society and were already expressed in the 1980s, even before the advent of the Internet. Thus, online communication tools are factors of propagation and dissemination of news and views. Although Algeria shares common cultural and social values and identities with countries where Arab Spring movements have been strong, “Internet revolution” has not taken place. Like all countries, Algeria has its own political model as well as a different and unique mentality.

Generalizations are (almost) always misleading; Internet and social media have not ultimately contributed to sustainably achieving Arab Spring objectives. In fact, excessive personalization and narcissistic exercise of power, the weakness of parliament, the vulnerability of political parties and the role of government are major obstacles to positive political change. More than that, political authorities are clinging to power; they themselves use Internet and social media to wage counter-revolutions through “electronic flies”. Practices of misuse, abuse, fake news and distortion of the truth now make the users doubtful and skeptical about the efficiency and reliability of Internet and social media in general. It appears that a “hidden and invisible hand” still continues to sow confusion and ambiguity.

Truth: The Arab Spring movement, if there ever was one beyond the Western narrative with this name, has neither resulted in newly democratized societies and nations states, nor did the upheavals have their origin in Internet or social media. Internet access and social media as platforms for awareness and organization have rather been supporting context factors for social unrest that yielded from deeply rooted wishes for (political) change.

Source

Kamal Eldin Osman Salih, The Roots and Causes of the 2011 Arab Uprisings, 35 Arab Studies Quarterly 35 (2013) 2, http://www.pinxit.com/page101/page115/downloads-23/files/Arab_Spring_Causes.pdf; George Lawson, Revolution, Non-Violence, and the Arab Uprisings, Mobilization: An International Quarterly (2015) 4, 453–470, http://eprints.lse.ac.uk/63156/1/Lawson_Revolution%2C%20non-violence.pdf.

MYTH #28

Das Internet fördert die Demokratie, so beispielsweise während des „Arabischen Frühlings“

Nein, sagt Laeed Zaghlami: Die Bewegung des Arabischen Frühlings, sollte es diese jemals jenseits des westlichen Narrativs mit dieser Bezeichnung gegeben haben, hat weder zu neu demokratisierten Gesellschaften und Staaten geführt, noch haben die Umbrüche ihren Ursprung im Internet oder in sozialen Medien. Internetzugang und soziale Medien als Plattformen für Aufklärung und Organisation bieten Raum zur Entfaltung von Kontextfaktoren für soziale Unruhen, die sich aus tief verwurzelten Wünschen nach (politischem) Wandel speisen.

الإنترنت تشجع الديمقراطية، كما حدث أثناء «الربيع العربي».

كلا، هكذا يقول العيد الزغلامي: لم يسفر حراك الربيع العربي - إذا كان هناك أصلاً حراك خارج نطاق السردية الغربية - عن مجتمعات ودول قومية حديثة الديمقراطية، كما أن نشأة هذه الاضطرابات لم تكن بدايتها على الإنترنت أو وسائل التواصل الاجتماعي. وبالأحرى لم يكن الوصول إلى الإنترنت ووسائل التواصل الاجتماعي كمنصات للتوعية والتنظيم سوى عوامل سياقية مساندة للقلاقل الاجتماعية التي نتجت عن رغبات عميقة الجذور في التغيير (السياسي).

互联网促进了民主，就像处于“阿拉伯之春”时代一样。

不，Laeed Zaghlami 写道：超越西方叙事的阿拉伯之春运动既未产生新成立的民主化社会和民族国家，也未起源于互联网或社交媒体。作为意识和组织平台，互联网接入和社交媒体相当支持社会动荡的背景因素，这些因素源于对（政治）变革的根深蒂固的愿望。

Internet favorise la démocratie, comme lors du « Printemps arabe ».

Non, écrit Laeed Zaghlami: le mouvement du Printemps arabe, s’il a jamais existé au-delà du discours occidental, n’a pas débouché sur des sociétés et des États-nations offrant une nouvelle démocratie, et les bouleversements ne trouvent pas non plus leur origine dans l’Internet ou les réseaux sociaux. L‘accès à Internet et les réseaux sociaux en tant que plateformes de parole et d‘organisation ont plutôt favorisé les facteurs contextuels de l‘agitation sociale qui découlaient de souhaits de changement (politique) profondément enracinés.

Интернет продвигает демократию, как во время «Арабской весны»

Это не так, говорит Лаид Заглами: Движение «Арабская весна», если когда-либо существовало движение с таким названием за пределами западной интерпретации, не привело к новым демократизированным обществам и национальным государствам, и эти потрясения не были порождены в Интернете или социальных сетях. Интернет-доступ и социальные сети как осведомительные платформы и организации скорее поддерживают контекстные факторы социальных волнений, вызванные укоренившимися желаниями (политических) перемен.

El internet promueve la democracia, como durante la “Primavera Árabe”.

No, dice Laeed Zaghlami: el movimiento de la Primavera Árabe, si es que realmente existió uno con este nombre más allá de la narrativa de Occidente, no ha resultado en nuevas sociedades democratizadas y Estados nacionales, y los levantamientos que ocurrieron en él tampoco tuvieron su origen en el internet o en las redes sociales. El acceso al internet y las redes sociales, como plataformas para la concienciación y la organización, más bien han estado apoyando factores contextuales de descontento social, derivados de voluntades de cambio (político) profundamente enraizadas.

MYTH #29

Franziska Oehmer and Stefano Pedrazzi

The Internet destroys the integrity of elections.

Myth: The Internet has become an increasingly important source of information for voters to form their opinions and interact with parties and candidates in elections. However, bots and trolls are suspected to massively manipulate the communicative process around voting and skew the actual popularity of certain politicians. This endangers the very basis for informed decision-making. The Internet thus destroys democratic elections and hijacks referenda.

Busted: Since the US election campaign and the Brexit vote in 2016, there has been speculation about the decisive influence of bots and trolls on online discourse. (→ #30) It is presumed that these (semi-)automated accounts that produce, distribute and like content or profiles in social networks under the pretense of human identity have distorted public opinion with serious consequences: Trump became president, and Great Britain decided to leave the EU.

The myth assumes, first, that bots and trolls quantitatively determine (or at least decisively influence) the political discourse by increasing the range of false news, inflating the popularity and relevance of political candidates, themes and positions, and making individuals and organizations of the political system or civil society disappear in the mass of communication activities or due to algorithmic filtering. It implies, second, that citizens mainly and uncritically rely on information from the Internet for their electoral decision.

The extent to which bots and trolls actually determine the discourse before elections and votes cannot be determined with absolute certainty. Depending on the vote, elections and national contexts, research has found different data and answers, ranging from comparatively large, yet not dominant, to negligibly small proportions of bot and troll accounts participating in the online discourse. The fluctuating values are also due to the fact that the identification of such accounts is (currently) difficult and unreliable. But even in the hypothetical case of stronger presence of bots and trolls in online political debates, it is unlikely that they will determine the decision at the ballot box. Only a small percentage of the population exclusively informs themselves via the Internet before elections or votes. (→ #23) In addition, having received information from the media or from unknown actors on the Internet is by no means the decisive predictor of the electoral decision: Rather, the personal exchange with our social environment or with recognized opinion leaders, as well as our existing political preferences, determine where we put the cross.

Truth: The Internet does not destroy democratic elections and votes. Currently, social bots and trolls have no dominant influence on opinion-formation and decision-making. Personal party preference and exchange with the social environment are still crucial. It cannot be ruled out, however, that the influence of bots and trolls may increase in the future.

Source

Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, Alessandro Flammini, The Rise of Social Bots, 59 Communications of the ACM (2016) 7, 96-104, https://dl.acm.org/citation.cfm?id=2818717; Samuel C. Woolley, Philip N. Howard (eds.), Computational Propaganda (Oxford: OUP, 2018).

MYTH #29

Das Internet verfälscht Wahlen.

Nein, sagen Franziska Oehmer und Stefano Pedrazzi: Das Internet verfälscht keine demokratischen Wahlen und Abstimmungen. Soziale Bots und Trolle haben derzeit keinen beherrschenden Einfluss auf Meinungsbildung und Entscheidungsfindung. Maßgeblich sind nach wie vor persönliche Präferenzen für eine politische Partei und der Austausch mit dem sozialen Umfeld. Es kann jedoch nicht ausgeschlossen werden, dass der Einfluss von Bots und Trollen in Zukunft zunehmen wird.

الإنترنت تدمر نزاهة الانتخابات.

كلا، هكذا يقول فرانسيسكا أومر وستيفانو بيدراتسي: لا تدمر الإنترنت الانتخابات والاقتراعات الديمقراطية، وليس للبوتات الاجتماعية ولا للمتصيدين في الوقت الراهن أي تأثير مُهيمن على تشكيل الرأي وصُنع القرار. وما زال التفضيل الحزبي الشخصي والتبادل مع البيئة الاجتماعية أمرًا بالغ الأهمية. ومع ذلك لا يمكن استبعاد أن يزداد تأثير البوتات والمتصيدين مستقبلاً.

互联网破坏了选举的完整性。

不，Franziska Oehmer 和 Stefano Pedrazzi 写道：互联网未破坏民主选举和投票。目前，社交网络机器人和网络喷子未对意见形成和决策产生主导性影响。个人偏好和与社会环境的交流仍然至关重要。但是，不能排除网络机器人和钓鱼的影响可能会在未来增加。

Internet détruit l‘intégrité des élections.

Non, écrivent Franziska Oehmer et Stefano Pedrazzi: Internet ne détruit pas les élections et les votes démocratiques. Actuellement, les robots sociaux et les trolls n‘ont aucune influence dominante sur la formation des opinions et la prise de décision. Les préférences personnelles en faveur de tel ou tel parti et les échanges avec le milieu social restent cruciaux. Cependant, on ne peut exclure que l‘influence des robots et des trolls augmente à l‘avenir.

Интернет губит честность выборов.

Это не так, говорят Франциска Омер и Стефано Педрацци: Интернет не сводит к нулю демократические выборы и голосования. На данный момент, социальные боты и тролли не имеют преобладающего влияния на формирование мнений и принятие решений. Определяющее значение все так же имеют персональные партийные предпочтения и обмен в социальном окружении. Однако нельзя исключать, что влияние ботов и троллей все же может возрасти в будущем.

El internet compromete la integridad de las elecciones.

democráticas y los votos. Actualmente, los bots y los trolls sociales no tienen una influencia dominante en la formación de las opiniones ni en la toma de decisiones. Las preferencias individuales de partidos y el intercambio con el entorno social siguen siendo cruciales en este sentido. No puede ser descartado, sin embargo, que la influencia de los bots y los trolls pueda aumentar en el futuro.

MYTH #30

Alek Tarkowski

Digital rights campaigns are run by bots, not real activists.

Myth: Like many other digital rights campaigns, the 2018/2019 protests against the EU Copyright Directive were not an expression of massive civic concern for digital rights. The protest campaign, the largest of its kind in recent years, was in fact a prime example of disinformation activities. It was a "fake grassroots uprising" by a small group of people who multiplied their numbers with the use of bots.

Busted: The suggestion that bots, and not humans, were responsible for many digital rights campaigns and especially the mass scale protests against the EU Copyright Directive originated with a group of artists rights' activists and lobbyists. The accusations were made without providing any evidence of actual mass-scale bot activity.

In an op-ed in the Frankfurter Allgemeine Zeitung on activism in "the time of the bots", the author argued that the 6 million calls and emails sent to the Members of European Parliament were largely automated. But many of those who argue that digital rights activism is run by bots confuse automation, which enables mass-scale online protests, with the use of "bots": fake accounts.

It is true that online campaigning systems used for the SaveYourInternet.eu campaign (and other campaigns conducted during the EU Copyright Directive policy process) automate elements of activism. A user of the campaign website can for example easily connect by phone - for free - with offices of multiple politicians or effortlessly promote the campaign through social media, using automatically generated messages and graphics. Such automation allows economies of scale and network effects to kick in, allowing the campaign to grow exponentially. Still, a human user is needed to make the call, send an email, or share information on social media. Critics of the campaign have not provided any evidence that among the millions of citizens supporting the campaigns were fake accounts, bots.

The allegations struck a cord among some of the politicians in Brussels. Members of Parliament complained that their mailboxes were flooded with copy-pasted messages. With no tools available to parse communication from their constituents happening at such massive scale, some of them apparently treated it as spam. This is why the negative PR spin fell on fertile ground. It fuelled a sense of disconnect between politicians and their voters in a system that does not provide meaningful ways of engagement between the two groups. Politicians ignored a simpler explanation: network effects (→ #41) made possible by digital communication tools make mobilization at the level of millions of citizens possible, at relatively low cost. European citizens simply care about online freedoms and are willing to protest against laws which they perceive as threatening those freedoms.

Furthermore, rights holders‘ lobbyists failed to mention that the same campaigning tools have been used on their side as well. As Corporate Europe Observatory notes, the real challenge has been the taking over of the public discussion by business lobbies representing big tech, publishers and collecting societies.

Truth: While automated campaigning tools have been employed to allow economies of scale and network effects to kick in, digital rights campaigns – such as the 2018 protests against the EU Copyright Directive – were supported by millions of humans, not bots, expressing their concern for online freedoms. Humans made calls, sent emails and shared information on social media – and protested on the streets with "We are not bots" becoming a successful slogan.

Source

Corporate Europe Observatory (2018), "Copyright Directive: how competing big business lobbies drowned out critical voices", https://corporateeurope.org/en/2018/12/copyright-directive-how-competing-big-business-lobbies-drowned-out-critical-voices; European Digital Rights (2018), Save Your Internet, https://saveyourInternet.eu.

MYTH #30

Kampagnen für digitale Rechte werden von Bots und nicht von realen Aktivist*innen durchgeführt.

Nein, sagt Alek Tarkowski: Zwar wurden durchaus automatisierte Kampagnenwerkzeuge eingesetzt, um Skalen und Netzwerkeffekte zu ermöglichen, jedoch wurden Kampagnen für digitale Rechte wie beispielsweise die Proteste gegen die EU-Urheberrechtsrichtlinie im Jahr 2018 nicht von Bots, sondern von Millionen von Bürger*innen in Sorge um die Freiheit des Internets unterstützt. Es waren Menschen, die anriefen, E Mails versandten, Informationen über soziale Medien teilten und mit dem Schlachtruf „Wir sind keine Bots" auf der Straße protestierten.

حملات الحقوق الرقمية تُدار على أيدي روبوتات لا ناشطين حقيقيين.

كلا، هكذا يقول أليك تاركوفسكي: على الرغم من استخدام أدوات تنظيم الحملات المؤتمتة للسماح بالاستفادة من وفورات الحجم وتأثيرات الشبكة، إلا أن حملات الحقوق الرقمية - كاحتجاجات ٢٠١٨ ضد توجيه الاتحاد الأوروبي لحقوق الطبع والنشر – ساندها ملايين البشر، لا الروبوتات، معربين عن قلقهم بشأن الحريات على الإنترنت. فالبشر هم الذين قاموا بإجراء المكالمات وإرسال الرسائل البريدية الإلكترونية وتشارُك المعلومات على وسائل التواصل الاجتماعي، واحتجوا في الشوارع مع تحول «لسنا روبوتات» إلى شعار ناجح.

数字版权运动由网络机器人（而非真正的活跃分子）操控。

不，Alek Tarkowski 写道：已采用自动化的竞选工具，使得规模经济和网络效应推动数字版权运动，例如 2018 年反对《欧盟版权指令》的抗议活动得到了数百万人（而非机器人）的支持，表明他们对网络自由的关注。人们在社交媒体上打电话、发电子邮件和共享信息，并在街头抗议，而且“我们不是机器人”成为响亮的口号。

Les campagnes pour les droits numériques sont gérées par des bots et non par de vrais activistes.

Non, écrit Alek Tarkowski: alors que des outils de campagne automatisés ont été utilisés pour permettre des économies d'échelle et des effets de réseau, les campagnes pour les droits numériques, telles que les manifestations de 2018 contre la directive européenne sur les droits d'auteur, ont été soutenues par des millions d'êtres humains, et non par des bots (robots informatiques), exprimant leur inquiétude vis-à-vis des libertés en ligne. Des humains ont passé des appels, envoyé des courriels et partagé des informations sur les réseaux sociaux, et ont protesté dans les rues avec le slogan à succès « Nous ne sommes pas des robots ».

Кампании по защите цифровых прав ведутся ботами, а не реальными активистами.

Это не так, говорит Алек Тарковски: В то время как автоматизированные агитационные инструменты использовались для активизации сетевых эффектов и эффекта масштаба, кампании по защите цифровых прав – такие как протесты против Директивы об авторском праве на Едином цифровом рынке ЕС в 2018 году – поддержали не боты, а миллионы людей, выражавших свою обеспокоенность в отношении свободы в Интернете. Люди совершали звонки, отправляли электронные письма, обменивались информацией в социальных сетях и протестовали на улицах, используя ставший популярным лозунг «Мы не боты».

Las campañas por los derechos digitales están dirigidas por bots y no por activistas reales.

No, dice Alek Tarkowski: mientras que las herramientas automatizadas de campaña se han utilizado para lograr efectos de economía de escala e interconexión, las campañas por los derechos digitales, tales como las protestas de 2018 contra la Directiva de la Unión Europea sobre derechos de autor, fueron apoyadas por millones de humanos, no bots, expresando sus preocupaciones con relación a las libertades digitales. Estos mismos humanos realizaron llamadas, enviaron emails y compartieron información en redes sociales, y hubo también protestas en las calles, convirtiéndose el famoso "No somos bots" en un eslogan exitoso.

MYTH #31

Sebastian Berg

The Internet enables organizing without organization.

Myth: The Internet provides a form of social and political organization without hierarchical and rigid structures. The reduction in communication and transformation costs resulting from digital technologies enables bottom-up networking, which makes institutional forms of politics obsolete, minimizes the exercise of power and brings about a radical democratic society.

Busted: The idea of the egalitarian and inclusive community is one of the founding myths of the Internet, as John Perry Barlow declared: "We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth" (Barlow 1996). (→ #28) From the beginning, it was assumed that the Internet provides tools or platforms that are easy to use and foster communication, thus naturally promoting the formation of new groups, mutual cooperation, and the possibility of participation without formal organization (Shirky 2008).

Although we have seen the disappearance of gatekeepers and instances in many areas, this does not apply to hierarchies and (political) institutions per se. As Melvin Kranzberg wrote, "Technology is neither good nor bad; nor is it neutral." It is open to design and reflects the conditions under which it is implemented. Every infrastructure must be operated, financed, and is integrated into given social structures so that "newer media practices in the interpenetrated fields of media and politics adapt and integrate the logics of older media practices" (Chadwick 2013). In fact, as the phrase "code is law" indicates (Lessig 1999) (→ #3), Internet based tools are by and large (material) institutions around which organization takes place. They have a structuring effect depending on the architecture of the platform and the social imaginaries according to which they are designed.

The myth has its origin in the "Californian Ideology", a combination of an anarchistic-alternative counterculture and libertarian technological utopia that rejects the need for formal power structures in favor of "unfettered interactions between autonomous individuals and their software" (Barbrook/Cameron 1996). It can be regarded as the founding myth of the Silicon Valley economy and has found global acceptance with the success of the large Internet companies (Turner 2006). However, this should not be equated with the current state of the Internet and the social appropriation of digital technology. Facing dubious proclamations about the importance "to develop the social infrastructure to give people the power to build a global community that works for all of us" (Zuckerberg 2017), we should not forget the fact that the Internet based platform economy is neither egalitarian nor exclusively bottom-up nor democratic, but characterized by centralization, institutionalization, and the establishment of new gatekeepers (van Dijck/Poell 2018). As technology always reflects the conditions of its social realization, we would rather benefit from ideological criticism than the spread of marketing myths.

Truth: Although we can observe a structural transformation in the way of political organization and connective forms of action supplement collective ones, so far existing (political) institutions such as the state, parties or companies remain in a privileged position to adapt to the affordances of digital technology. Digital instruments are used to make organizations more inclusive and reduce old barriers, but they will not replace organizations and politics.

Source

Clay Shirky, Here Comes Everybody. The Power of Organizing without Organization (London: Penguin Books, 2008); Fred Turner, From Counterculture to Cyberculture (Chicago/London: University of Chicago Press, 2006).

MYTH #31

Das Internet ermöglicht Organisation ohne Organisation.

Nein, sagt Sebastian Berg: Auch wenn wir einen strukturellen Wandel in der Art der politischen Organisation beobachten können und konnektive Handlungsformen kollektiv ergänzen, sind bisher bestehende (politische) Institutionen wie der Staat, Parteien oder Unternehmen nach wie vor besser in der Lage, sich an die Fortschritte der digitalen Technologie anzupassen. Digitale Instrumente werden eingesetzt, um Organisationen integrativer zu machen und alte Barrieren abzubauen, aber sie werden Organisationen und die Politik nicht ersetzen.

الإنترنت تتيح التنظيم من دون منظمات

كلا، هكذا يقول سيباستيان بيرغ: مع أننا نلاحظ تحولاً هيكليًّا فيما يضيفه التنظيم السياسي وطرق العمل الرابط إلى أشكالَ العمل الجماعي، ما زالت المؤسسات (السياسية) الموجودة، كالدولة أو الأحزاب أو الشركات، في وضع مواتٍ للتكيف مع موارد التكنولوجيا الرقمية. وتُستخدم الأدوات الرقمية لجعل المنظمات أكثر شمولاً ولتقليص الحواجز القديمة لكنها لن تحل محل التنظيمات والسياسة.

互联网使得无组织的组织成为可能

不，Sebastian Berg 写道：虽然我们可以察觉到政治组织方式的结构转型，而且行动的连接形式也对集体形式进行了补充，但到目前为止，现有的（政治）机构，如国家、政党或公司，仍在适应数字技术的功能可承受性方面享有特权。数字仪表用于使组织更具包容性并减少以往的障碍，但它们不会取代组织和政治。

Internet permet d‘organiser sans organisation.

Non, écrit Sebastian Berg: bien que nous assistions à une transformation structurelle de la manière dont l‘organisation politique et les formes d‘action « connectives » complètent les actions « collectives », les institutions (politiques) existantes telles que l‘État, les partis ou les entreprises restent jusqu‘à présent dans une position privilégiée pour s‘adapter aux avantages du numérique. Les instruments numériques sont utilisés pour rendre les organisations plus inclusives et réduire les anciens obstacles, mais ils ne remplaceront pas les organisations et la politique.

Интернет можно организовать без организации

Это не так, говорит Себастьян Берг: Хотя мы можем наблюдать структурное преобразование способа политической организации и связывающие меры, дополняющие коллективные, до сих пор существующие (политические) институты, такие как государство, партии или компании сохраняют привилегированное положение в плане приспособления к возможностям цифровых технологий. Цифровые инструменты используются для того, чтобы сделать организации более всесторонними и стереть старые барьеры, но они не заменят организации и политику.

El internet permite una organización sin organización.

No, dice Sebastian Berg: aunque es posible observar una transformación estructural en la forma en que la organización política y las formas conectivas de acción se complementan con las colectivas, las instituciones (políticas) existentes tales como el Estado, los partidos y las compañías mantienen una posición privilegiada para adaptarse a las potencialidades de la tecnología digital. Los instrumentos digitales son utilizados para hacer a las organizaciones más inclusivas y para reducir viejas barreras, pero no reemplazarán a las organizaciones ni a la política.

MYTH #32

Fabian Ferrari and Mark Graham

Digital work is immaterial.

Myth: Governments, philanthropists, companies and supranational organizations around the globe pitch digital work as an economic boost for rural and economically marginalized areas. A key element of these optimist discourses is the presumed aspatial and immaterial nature of digital work. Because of the immateriality of the Internet, work can now be done from anywhere.

Busted: Work, and the networks that extract value from it, are increasingly embedded into planetary systems. As ever more work is commodified and traded beyond local labour markets, the hidden digital supply chains spanning our planet purport to pay little attention to the locations in which work is done.

Workers embedded into digital production networks produce immaterial outputs. These outputs can be instantly transmitted anywhere on the planet. This means that for work that relies on the production and processing of codified rather than tacit knowledge, proximity is no longer needed between workers and the objects and subjects of their work.

For many commentators, the fact that Amazon contractors in Romania listened to Alexa conversations or that Facebook commissioned Indian contractors to read private messages of users is a violation of the right to privacy. (→ #45) However, beyond privacy concerns, these cases are exemplary of a planetary network of extracting cognitive labour that happens in real-time.

Work, in other words, can be deterritorialized at a planetary scale. This is not an argument that geography no longer matters. Far from it. Networks of production settle precisely in the places with the most advantageous political economies. Contemporary digital production networks attempt to integrate production that is algorithmically and manually produced.

In the history of capitalism, it is not a new phenomenon that production networks of commodities are not visible to consumers. But with immaterial goods like face recognition softwares or speech assistants it is not even possible to gaze backwards in the chain of production in the same way as with coffee or chocolate because these systems are always unfolding and never fixed in nature. To a certain degree, AI systems are technical illusions, always in a state of becoming rather than a static state of being, with many workers fixing and tweaking their shortcomings. What is being pitched as AI innovations is often the combined effort of cognitive work by many underpaid human workers. (→ #43)

Taking seriously the materiality of digital work enables us to ask important questions aimed at understanding the relative embedded- and disembedded, material and immaterial, and territorialized and deterritorialized natures of digital production.

Truth: Digital work is impossible to conceptualize in isolation from the infrastructures that mediate, augment, and extract value from it. Production networks that fuse automated systems and human production create different forms of value; and, despite their seeming immateriality, they use and engender particular economic geographies.

Source

Mark Graham, Isis Hjorth and Vili Lehdonvirta, Digital labour and development: impacts of global digital labour platforms and the gig economy on worker livelihoods. Transfer: European Review of Labour and Research, 23 (2017) 2, 135-162; Mark Graham and Mohammad Amir Anwar, The Global Gig Economy: Towards a Planetary Labour Market? First Monday 24 (2019) 4, doi.org/10.5210/fm.v24i4.9913.

MYTH #32

Digitale Arbeit ist immateriell.

Nein, sagen Fabian Ferrari und Mark Graham: Digitale Arbeit kann unmöglich getrennt von den Infrastrukturen konzeptualisiert werden, die Werte vermitteln, steigern und extrahieren. Produktionsnetzwerke, bei denen automatisierte Systeme und menschliche Produktion verschmolzen sind, schaffen verschiedene Formen von Wert; und trotz ihrer scheinbaren Immaterialität nutzen und erzeugen sie bestimmte geografische Wirtschaftsräume.

العمل الرقمي غير مادي.

كلا، هكذا يقول فابيان فيراري ومارك غراهام: يستحيل تصوّر العمل الرقمي بمعزل عن البنى التحتية التي تؤثر عليه وتُعززه وتستخلص منه القيمة. فشبكات الإنتاج التي تدمج النُظم المؤتمتة والإنتاج البشري تخلق أشكالاً مختلفة من القيمة؛ وعلى الرغم من طبيعتها غير المادية ظاهريًّا، إلا أنها تَستخدم وتولّد جغرافيات اقتصادية معينة.

数字化工作不重要。

不，Fabian Ferrari 和 Mark Graham 写道：数字化工作不可能从调解、增强和从中提取价值的基础设施中脱离出来并概念化。融合自动化系统和人类生产的生产网络创造不同形式的价值，尽管它们看起来不重要，但它们使用并产生了特定的经济地理。

Le travail numérique est immatériel.

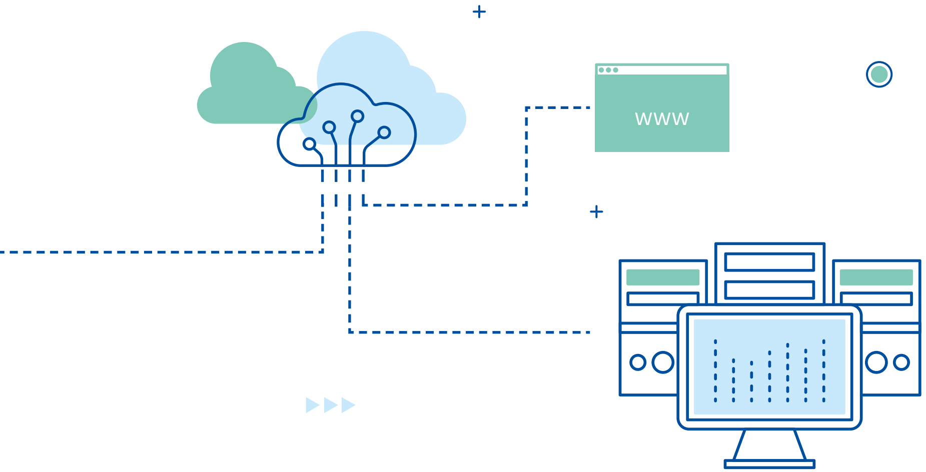
Non, écrivent Fabian Ferrari et Mark Graham: il est impossible de conceptualiser le travail numérique indépendamment des infrastructures qui le servent, le complètent et en tirent de la valeur. Les réseaux de production qui combinent systèmes automatisés et production humaine créent différentes formes de valeur et, malgré leur apparente immatérialité, ils utilisent et créent des zones géographiques économiques particulières.

Цифровая сеть нематериальна.

Это не так, говорят Фабиан Феррари и Марк Грэхэм: Цифровую деятельность невозможно осмыслить в отрыве от инфраструктур, которые являются ее посредниками, увеличивают и извлекают из нее ценность. Производственные сети, объединяющие автоматизированные системы и человеческое производство, создают различные формы ценности; и, несмотря на их видимую нематериальность, они используют и порождают особую экономическую географию.

La obra digital es inmaterial.

No, dicen Fabian Ferrari y Mark Graham: la obra digital es imposible de conceptualizar sin considerar las infraestructuras que median, aumentan y extraen valor de ella. Las redes de producción que aúnan los sistemas automatizados y la producción humana producen tipos de valor distintos y, a pesar de su aparente inmaterialidad, generan y utilizan geografías económicas particulares.



CHAPTER 4

Infrastructure and innovation

Infrastruktur und Innovation

الإدماج والتكامل

基础设施与创新

Infrastructure et innovation

Инфраструктура и инновации

Infraestructura e innovación

MYTH #33

Daniel Lambach

Cyberspace is totally separate from “the real world”.

Myth: Founded on a logic of Internet exceptionalism, “the Internet” represents a space that is distinct from the “real world”. “Cyberspace” and “meatspace” are two different worlds and they are, or at least should be, governed by different logics, structures, norms and actors.

Busted: Artistic renderings of cyberspace depict it as a singular space with its own topography and boundaries, maybe as a continent, a subway grid or a network cloud. (→ #35; → #37) Implicit in these depictions is the assumption that cyberspace – as a space – is distinct from the “real world”. Nowhere has this been more forcefully expressed than in the Declaration of the Independence of Cyberspace (Barlow 1996), which boldly intones: “Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind.” The techno-utopians liked to refer to cyberspace as the “electronic frontier”, deliberately invoking the imagery of the settling of the American Frontier as a land of opportunity, free from governmental interference. Such spatial metaphors are still very common. Angela Merkel famously referred to the Internet as “Neuland” (“uncharted territory”). With our cognition centered around three-dimensional vision, spatial metaphors come to us naturally. Certainly, spatial ways of imagining cyberspace clash with the Internet’s network structure although they are no less powerful because of that (Lambach 2019).

But such a way of thinking cyberspace has two important flaws. First, cyberspace is not a singular place, a flat expanse of electronic terrain. Instead, it is a complex set of “cyber-territories” constructed by states, corporations and users. States create “national segments” of the Internet through e.g. data localization laws, parallel addressing infrastructures and robust cyber defense doctrines. (→ #38). Corporations create walled gardens or ecosystems wherein they sell their product or sell users’ attention to advertisers under their internal standards and content management policies. Users create small and adaptable territories through online communities or chat groups. These territories overlap, conflict and shift. Normative conflicts abound: there are, for instance, many ways to approach legal liability for online speech at the intersection of state and corporate online “territories” (→ #6).

Second, the distinction between “online” and “offline” space is breaking down, if it ever was true. Cyberspace can be brought into the “real world” through smartphones, optical displays, IoT devices and other ever more ubiquitous artefacts. Social communication becomes an ever more entangled complex of technologically mediated contacts and face-to-face interaction. The “real world” is brought into cyberspace through geolocation technologies which are fundamentally changing the character of the Internet. These trends are integrating physical location and online spaces into one emerging, hybridized whole, further undercutting the premise of Internet exceptionalism.

Truth: Cyberspace is not a singular space but a set of overlapping, conflicting and shifting “cyber-territories”. Furthermore, the division of cyberspace and the “real”/offline world is becoming less and less tenable as computing becomes more ubiquitous. The Internet is not an exceptional space after all.

Source

John Perry Barlow, A Declaration of the Independence of Cyberspace (1996), https://projects.eff.org/~barlow/Declaration-Final.html; Daniel Lambach, The Territorialization of Cyberspace, International Studies Review (2019), https://doi.org/10.1093/isr/viz022 or https://www.researchgate.net/publication/308720083_The_Territorialization_of_Cyberspace (ungated preprint).

MYTH #33

Der Cyberspace ist ein von der „realen Welt“ vollkommen losgelöster Raum.

Nein, sagt Daniel Lambach: Der Cyberspace ist kein singulärer Raum, sondern vielmehr eine Reihe sich überschneidender, widersprüchlicher und sich verschiebender „Cyberterritorien“. Darüber hinaus wird die Trennung von Cyberspace und „realer“/Offline-Welt mit zunehmender Allgegenwärtigkeit des Computers immer obsoleter. Das Internet ist letztlich doch kein abgrenzbarer Raum.

الفضاء السيبراني فضاء منفصل عن «العالم الحقيقي».

كلا، هكذا يقول دانيال لامباخ: الفضاء السيبراني ليس مساحة أحادية بل مجموعة من «المناطق السيبرانية» المتداخلة والمتضاربة والمتغيرة. علاوة على ذلك فقد أصبح تقسيم الفضاء السيبراني والعالم «الحقيقي» غير المتصل بالإنترنت أقل قابلية للتطبيق مع اتساع انتشار الحوسبة. فالإنترنت ليست فضاءً استثنائيًّا في نهاية المطاف.

网络空间是一个与“现实世界”分离的空间。

不，Daniel Lambach 写道：网络空间不是一个奇异空间，而是一系列重叠、冲突和变化的“网络领域”。此外，随着计算变得越来越无处不在，网络空间和“真实”/线下世界的划分变得越来越不合理。毕竟，互联网并非特殊的空间。

Le cyberespace est un espace séparé du « monde réel ».

Non, écrit Daniel Lambach: le cyberespace n‘est pas un espace singulier, mais un ensemble de « cyber-territoires » se chevauchant, en conflit et en mutation. En outre, la dichotomie entre cyberespace et monde « réel »/hors-ligne devient de moins en moins tenable à mesure que l‘informatique devient plus omniprésente. Finalement, Internet n‘est pas un espace exceptionnel.

Киберпространство отделено от реального мира.

Это не так, говорит Даниэль Ламбах: Киберпространство – это не единичное пространство, а набор пересекающихся, сталкивающихся и перемещающихся «кибертерриторий». К тому же, разделение киберпространства и «реального» / офлайн мира становится все менее устойчивым, поскольку информационные технологии распространяются все шире. В конце концов, Интернет не является исключительным пространством.

El internet es un espacio disociado del “mundo real”.

No, dice Daniel Lambach: el ciberespacio no es un espacio único, sino un conjunto de “ciberterritorios” superpuestos, en conflicto y cambiantes. Además, la división entre el ciberespacio y el mundo “real” (offline) está volviéndose cada vez menos tangible, a medida que la tecnología computacional se hace más y más omnipresente. El internet no es un espacio excepcional a fin de cuentas.

MYTH #34

Martin Dittus, Sanna Ojanperä and Mark Graham

There is no “there” on the Internet.

Myth: The Internet is a “global village”, shrinking the world down to a single global marketplace and social sphere, where everyone meets and all have access to the same services. This “virtual world”, this cyberspace, is one shared place that is separate from all the places in the real world.

Busted: Today, we can no longer say that the “virtual” is clearly distinguishable from the “real”, the “offline” from the “online”. (→ #33). Now that over half the world‘s population is connected to the Internet, most of our lives are accompanied by digital information overlays that augment our daily experience that shapes our understanding of the world and our actions in the world, no matter where in the world we are. In part this expansion of global connectivity is the result of spatial processes: through construction of new underwater cables connecting continents, and new regional networks providing broadband to homes and workplaces.

At the same time, many global regions remain disconnected, in particular rural and remote areas. Further, there is stark global inequality in the cost of connectivity (→ #36): in many countries, the cost of broadband still exceeds the monthly average salary. As a result of these barriers we see a global imbalance in potential digital participation, which is an imbalance in the capacity to participate in and shape life online. The resulting feedback loops produce inequalities in coverage: for many regions in the world, digital information on online knowledge platforms is still not available in a local language. For example, despite Wikipedia‘s best efforts and its 300 language editions, its most detailed representations of countries in the Global South are often written in a non-local language, typically English, and its content about the Global South is often produced by editors in North America and Europe. (→ #18)

To an extent these digital divides reflect existing economic divides. (→ #39) At the same time, where the early Internet was once predominantly in North America, we now see the emergence of a pluriverse of parallel digital cultures. In many of the world’s regions, platforms have emerged that are not part of the Western canon. This includes WeChat and Alibaba in China, Grab and Shopee in South East Asia, Flipkart and Reliance Jio in India, MercadoLibre and Universo Online in Latin America, and many more. In the near future we can anticipate further growth in non-Western digital participation, with Asia as the key driver, and Africa showing significant potential for further growth. Conversely, the “global” platform behemoths of Google, Apple, Facebook, Amazon, Netflix and others may find it increasingly hard to adapt to some of these emerging markets.

Truth: The Internet is not a global village, rather, it is a network that augments life in many places. If we want to understand what “the Internet” looks like, we need to be fluent in at least dozens of global cultures. Internet researchers are only ever researching particular digital neighborhoods. Distance still matters, and it will continue to do so.

Source

Mark Graham, Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities?, The Geographical Journal, 179(2) (2013), 177–182, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2166874; Sanna Ojanperä, Mark Graham, Ralph Straumann, Stefano De Sabbata, Matt Zook, The Geography of Engagement in the Knowledge Economy: Regional Patterns of Content Creation, Information Technologies in International Development 13 (2017), 33–51; https://lra.le.ac.uk/handle/2381/40079

MYTH #34

Es gibt kein „dort“ im Internet.

Nein, sagen Martin Dittus, Sanna Ojanperä und Mark Graham: Das Internet ist kein globales Dorf, sondern ein Netzwerk, das das Leben an vielen Orten bereichert. Um zu verstehen, wie „das Internet“ aussieht, müssen wir mit Dutzenden globalen Kulturen vertraut sein. Internetforscher betrachten immer nur bestimmte digitale Umgebungen. Entfernung spielt nach wie vor eine Rolle, und dies wird auch künftig so bleiben.

لا يوجد ما يدعى «هناك» على الإنترنت.

كلا، هكذا يقول مارتن ديتوس وسانا أوجانبيرا ومارك غراهام: الإنترنت ليست قرية عالمية، بل بالأحرى شبكة تُعزز الحياة في أماكن كثيرة. ولو أردنا فهم كيف تبدو «الإنترنت»، فلا بد أن نكون على دراية تامة بعشرات الثقافات العالمية على الأقل. وكل ما يفعله باحثو الإنترنت هو إجراء بحث يغطي مناطق محلية رقمية معينة. فالمسافة ما زالت وستبقى مهمة.

互联网上没有“边界”。

不，Martin Dittus, Sanna Ojanperä 和 Mark Graham 写道：互联网不是一个地球村，而是一个改善很多地方生活的网络。如果我们想要了解“互联网”，我们需要至少精通数十种全球文化。互联网研究人员从来只研究特定的数字社区。距离仍然很重要，并将继续存在。

Il n‘y a pas de « là » sur Internet.

Non, écrivent Martin Dittus, Sanna Ojanperä et Mark Graham: Internet n‘est pas un village global, mais un réseau qui améliore la vie dans de nombreux endroits. Si nous voulons comprendre à quoi ressemble Internet, nous devons maîtriser au moins des dizaines de cultures différentes. Les personnes effectuant des recherches sur Internet ne font que chercher dans des quartiers numériques particuliers. La distance compte encore, et comptera toujours.

В Интернете не существует понятия «там».

Это не так, говорят Мартин Диттус, Санна Оянперя и Марк Грэм: Интернет – это не всемирная деревня, скорее, это сеть, которая дополняет жизнь во многих местах. Если мы хотим понять, что «Интернет» из себя представляет, нам нужно знать тонкости как минимум десятка мировых культур. Интернет-исследователи фокусируются только на отдельных цифровых областях. Расстояние по-прежнему важно, и будет таковым.

No existe un “ahí” en el internet.

No, dicen Martin Dittus, Sanna Ojanperä y Mark Graham: el internet no es una aldea global; es, más bien, una red que complementa la vida en muchos lugares. Si queremos saber cómo se ve “el internet”, necesitamos tener un conocimiento profundo de al menos una docena de culturas globales. Los estudiosos del internet solamente investigan vecindarios digitales específicos. La distancia aún juega un papel importante y continuará haciéndolo.

MYTH #35

Sebastian Gießmann

The Internet is an Internet.

Myth: The Internet is a "network of networks". It connects heterogeneous elements, not just technically, but also socially and economically. This set-up ensures universal connectivity and interoperability and has implications for peer-to-peer networking approaches and ideals for realizing democratic values in a network of equals.

Busted: The Internet we have is not an Internetwork of heterogeneous networks, as counterintuitive as it might seem. Network protocols are infrastructure, and infrastructure is boring, bureaucratic and usually taken for granted. Yet developers and administrators of network protocols know about the social and relational character of digital infrastructure, and what is at stake politically in the design of network protocols (→ #4). In a 2006 interview, computer scientist David Reed made some 1980s political choices of protocol developers transparent: "In fact, the idea of pursuing a thing called 'the Internet' (an ur-network-of-networks) was a political choice – that universal interoperability was achievable and desirable. It's parallel to 'One Europe' or 'World Government', though not the same. The engineers involved were not ignorant of the potential implications at the political level of that choice" (Reed in Gillespie 2006, 452). Reed's argument is somewhat typical of the values that influenced the design of Internet protocols and its end-to-end architecture. It also misses one important historical point.

"Universal interoperability" depends on standardization, and network protocols form the de facto standards of digital mediation. On 1 January 1983, TCP/IP, the Transmission Control Program and Internet Protocol were imposed as a standard by the US Department of Defense. US universities followed that directive and gladly adopted TCP/IP. What did that transition within the ARPAnet achieve? Computer scientist John Day argues that within that infrastructural shift the Internetworking layer actually got lost. Picture Day's central argument not in all its subtlety, but in its consequences when he asks "How in the heck do you lose a layer?". He stresses that the split of TCP and IP "contributed to being an Internet in name only" (Day 2013, 22).

Open Systems Interconnection (OSI) and other internetworking approaches took into account that interconnected networks could be based on completely different technologies and addressing schemes (→ #15). But the Internet Protocol created only one address space for all connected networks; and today's Domain Name System has been built along that path dependency (→ #38). You can still hook up any other network with obscure protocols to the Internet as long as it uses the ruling IP addressing system. The 1990s slogan "IP on everything" did not create an ur-network-of-networks. It rather reinforced the loss of what would have been an internetworking layer in a scientifically sound and technically interoperable network architecture. Currently, we need to live with that flaw. The Internet is not a space for heterogeneous networking of heterogeneity that so many people still think: "OSI had an Internet Architecture and the Internet has a Network Architecture" (Day 2012, 15).

Truth: Ever since the internetworking layer got lost in 1983, the Internet's architecture depends on a homogeneous system of naming and addressing. The domain name system DNS does exactly that, creating one seamless space for IP addresses that needs to be centrally administered, even if domain registration procedures are decentralized. The current Internet does not interconnect completely heterogeneous networks, but remains just one single network on the level of naming and addressing. So when will we have a real Internetwork?

Source

John Day, How in the Heck Do You Lose a Layer!?, Future Network Architectures Workshop University of Kaiserslautern, 2012, https://www.researchgate.net/publication/261458332_How_in_the_Heck_do_you_lose_a_layer and John Day, Surviving Networking's Dark Ages or How in the Hell Do You Lose a Layer!? (IRATI RINA Workshop, Barcelona, 2013), http://irati.eu/wp-content/uploads/2013/01/1-LostLayer130123.pdf; Tarleton Gillespie, Engineering a Principle: "End-to-End" in the Design of the Internet, Social Studies of Science 36 (3) (2006), 427–457.

MYTH #35

Das Internet ist ein Internet.

Nein, sagt Sebastian Gießmann: Seitdem die Internetworking-Schicht 1983 verloren ging, hängt die Architektur des Internets von einem homogenen Namensgebungs und Adressierungssystem ab. Das Domain-Name-System DNS tut genau das und schafft einen nahtlosen Raum für IP-Adressen, der zentral verwaltet werden muss, auch wenn die Domainregistrierung dezentral erfolgt. Das heutige Internet verbindet keine völlig heterogenen Netzwerke, sondern bleibt ein lediglich auf Namensgebungs und Adressierungsebene beruhendes Netzwerk. Wann bekommen wir also echtes Internetworking?

الإنترنت هي شبكة شابكة.

الإنترنت هي شبكة شابكة.

كلا، هكذا يقول سيباستيان غيسمان: الإنترنت التي لدينا ليست «شبكة شبكات». كما أنها ليست شبكة بينية من الشبكات غير المتجانسة. وبالتالي فهي ليست إنترنت بالمعنى الحقيقي للكلمة. ومنذ عام ١٩٨٣ ظلت شبكة واحدة على مستوى التسمية والعنونة.

互联网是一种互联网络。

不，Sebastian Gießmann写道：我们拥有的互联网不是“网络之网”，也不是异构网络的互联网，因此，不是真正意义上的互联网。自1983年以来，互联网在命名和寻址方面始终保持单一网络。

Internet est un interréseau.

Non, écrit Sebastian Gießmann: l'Internet dont nous disposons n'est pas un « réseau de réseaux ». Ce n'est pas non plus un interréseau de réseaux hétérogènes. Par conséquent, ce n'est pas un Internet au vrai sens du mot. Depuis 1983, il est resté un réseau unique en termes de noms et d'adresses.

Интернет – это интернет.

Это не так, говорит Себастьян Гиссманн: Интернет, которые у нас есть – это не «сеть сетей». А также и не сеть, состоящая из неоднородных сетей. А следовательно это не Интернет в истинном смысле этого слова. С 1983 года он остается всего одной сетью на уровне присвоения имени и адресации.

El internet es un solo internet.

No, dice Sebastian Gießmann: el internet que tenemos no es una “red de redes”. Tampoco es una interred de redes heterogéneas. Es decir, no es un “internet” (interred) en el sentido estricto del término. Ya desde 1983, el internet ha sido una red única solamente a nivel de nombre y sistema de direcciones.

MYTH #36

Bob Frankston

We pay to access the Internet, which is provided by others.

Myth: We treat the Internet as a service we get from a provider or as a place we access. We subscribe, pay to access the Internet and worry about using up data quotas.

Busted: In the spring of 1973, I happened to take a class in which I learned about ALOHAnet in Hawaii, which consisted of just computers and radios. If a packet was lost, the program in your computer would just resend it. A classmate, Bob Metcalfe, used this idea as the basis for his famous networking technology, Ethernet. By the 1960's computers were fast enough so that we didn't need to rely on services from a carrier and, if packets were lost, we could quickly resend them. Or we could do streaming and ignore lost packets.

It was not until the 1990's when I was working on home networking at Microsoft that I fully appreciated that these were not networks in the traditional sense of being one service that assures your messages get through in the same way a railroad assures you your package will reach its destination.

I've been fortunate to have friends and colleagues who were tasked with internetworking disparate networks and recognized the power of this technique. The name "Internet" stuck, yet it was no longer a network but rather a way to use existing facilities without depending on a carrier. This allowed the disparate networks to use all available infrastructures including existing telecom facilities and meld them into a common inter-network. The Internet isn't a place but rather the way we use any available facilities (→ #35).

Physical analogies fail us when we think of data being sent as freight: Unlike a traditional network we do not necessarily send data ("content") but rather a reference such as a URL (reference) to a web page. We use this same idea when placing an order with Amazon and it sends the part number to the nearest warehouse instead of shipping from Seattle.

Thanks to using common protocols, the individual efforts can composite into the whole we call "the Internet". It is not provided but rather emerges out of the shared effort. It is not limited by how much data we can put through a pipe, but rather it grows as we contribute new ideas and make new facilities available.

Truth: The Internet is the way we use our wires and radios and not a service we buy. When we buy a broadband connection, we are paying to get past a gatekeeper. That is not paying for the Internet but getting past a legacy paywall. We need an Internet-native infrastructure.

Source

Jerry H. Saltzer, David P. Reed and David D. Clark, End-to-end Arguments in System Design, ACM Transactions on Computer Systems (TOCS) 2 (1984) 4, 277-288, http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf; Calvin Hennick, How ALOHAnet Helped Hawaii Make Waves in Networking and IT Innovation, StateTech, 30 June 2016, https://statetechmagazine.com/article/2016/06/how-alohanet-helped-hawaii-make-waves-networking-and-it-innovation.

MYTH #36

Wir bezahlen für den Zugang zum Internet, das von anderen zur Verfügung gestellt wird.

Nein, sagt Bob Frankston: Das Internet ist die Art und Weise, wie wir unsere Kabel und Funkverbindungen nutzen, und nicht ein Service, den wir kaufen. Wenn wir eine Breitbandverbindung buchen, bezahlen wir, um an einer Schranke vorbeizukommen. Wir bezahlen also nicht für das Internet, sondern um eine künstlich errichtete Paywall zu passieren. Wir brauchen eine internet-native Infrastruktur.

ندفع المال للوصول إلى الإنترنت التي يوفرها الآخرون.

كلا، هكذا يقول بوب فرانكستون: الإنترنت هي الطريقة التي نستخدم بها أسلاكنا وأجهزتنا وليست خدمة نشتريها. عندما نشتري وصلة عريضة النطاق فنحن ندفع المال للمرور من حارس بوابة. هذا لا يعني أننا ندفع مقابل الإنترنت بل ندفع من أجل الولوج عبر بوابة الاشتراك. نحن بحاجة إلى بنية تحتية محلية للإنترنت.

我们可付费访问他人提供的互联网。

不，Bob Frankston 写道：互联网是我们使用电线和无线电（而非我们购买的服务）的方式。当我们购买宽带连接时，我们其实是在花钱请一个看门人。这不是支付互联网费用，而是按照传统付费墙的标准付费。我们需要互联网“土生土长”的基础设施。

Nous payons pour accéder à Internet fourni par d‘autres.

Non, écrit Bob Frankston: Internet est la façon dont nous utilisons les câbles et les ondes et non un service que nous achetons. Lorsque nous nous abonnons à une connexion haut débit, nous payons pour passer un contrôle d‘accès. Ce n‘est pas payer pour Internet, mais pour accéder au-delà d’un système de paiement dépassé. Nous avons besoin d‘une infrastructure native pour Internet.

Мы платим за доступ к Интернету, который предоставляется другими.

Это не так, говорит Боб Франксон: Интернет – это способ, с помощью которого мы используем наши провода и радио, а не услуга, которую мы покупаем. Приобретая высокоскоростное подключение, мы платим, чтобы обойти контроллер. Это не плата за Интернет, а преодоление унаследованной системы, предусматривающей платный доступ к информации. Нам нужна естественная Интернет-инфраструктура.

Pagamos para acceder al internet que nos proporcionan otros.

No, dice Bob Frankston: el internet es la forma en la que utilizamos nuestros cables y radios y no un servicio que compramos. Cuando pagamos por una conexión de banda ancha, estamos pagando por un pasaporte para cruzar por una aduana digital. No estamos pagando por el internet, sino para pasar a través de un muro de pago. Necesitamos una infraestructura para el acceso nativo al internet.

MYTH #37

Daniel Voelsen

The Internet is in the clouds.

Myth: The Internet frees us from the limitations of physical space. Our data is in “the cloud”, where we can access it from anywhere, anytime, often using wireless mobile devices. Our communication thus transcends the old Westphalian order of territorially defined states.

Busted: The Internet depends on a massive physical infrastructure: More than 90% of all global Internet traffic today is routed through undersea cables. The many online services we use every day, including the different “cloud” services, require massive data centres. And our smartphones would turn out to be quite unhelpful without a dense net of mobile network infrastructure that connects them with the global Internet.

For the most part, this infrastructure is owned and operated by private companies. It is not a surprise, thus, that its development is shaped quite substantially by economic considerations. In particular, private companies invest more extensively in areas that promise greater returns: In many states, urban areas are thus often better connected than rural areas, and economically thriving states have more and stronger links to the global web than developing states (→ #39).

In a very fundamental sense, moreover, the Internet’s physical infrastructure ties it to the Westphalian world order of territorially defined statehood. All cable connections, wireless stations routers, Internet Exchange Points (IXPs), data centers and servers have a physical location and thus are subject to the jurisdiction of the respective states. The only exception to this are those parts of undersea cables that run on the high seas and the satellites that travel in outer space.

Ever more states seek control over the physical infrastructure of the Internet as a means to more effectively govern what they perceive as “their” parts of the Internet. One of the most brute approaches is to force telecommunication companies to limit or completely shut down Internet access in order to suppress the exchange of information between citizens. In a more sophisticated fashion, a number of states attempt to control in a more detailed manner what information enters, or leaves, their territory. They do so, for instance, by limiting the nodes that connect domestic Internet users with the global web, and then using different filtering mechanisms to block unwanted information. “Data localization” laws are another means by which states try to consolidate control over the physical infrastructures; the idea here is to make access to a state’s market conditional on storing the data of customers on the respective state’s territory.

Truth: The Internet depends on a complex global infrastructure. In addition to the logical layer of software standards and protocols, this infrastructure includes physical components, such as undersea cables and data centers. This physical layer inevitably ties the Internet to the world of territorial states – and therefore should receive more attention.

Source

Tara M. Davenport, Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, Catholic University Journal of Law and Technology 24 (2015), https://scholarship.law.edu/jlt/vol24/iss1/4; Laura DeNardis, Hidden Levers of Internet Control. An Infrastructure-Based Theory of Internet Governance, Information, Communication & Society 15 (2012) 5, 720-738, https://www.tandfonline.com/doi/full/10.1080/1369118X.2012.659199.

MYTH #37

Das Internet existiert nur in den Clouds.

Nein, sagt Daniel Voelsen: Das Internet ist auf eine komplexe globale Infrastruktur angewiesen. Neben der logischen Ebene von Softwarestandards und Protokollen umfasst diese Infrastruktur auch physische Komponenten wie beispielsweise Seekabel und Rechenzentren. Diese physische Ebene verbindet das Internet zwangsläufig mit der Welt der Territorialstaaten und verdient daher mehr Aufmerksamkeit.

الإنترنت في السحاب.

كلا، هكذا يقول دانيال فويلسن: تعتمد الإنترنت على بنية أساسية عالمية معقدة. وبالإضافة إلى الطبقة المنطقية المتمثلة في معايير وبروتوكولات البرمجيات، تشمل هذه البنية التحتية مكونات مادية كالكابلات البحرية ومراكز البيانات. هذه الطبقة المادية تربط الإنترنت حتمًا بعالم الدول الإقليمية وبالتالي يجب أن تحظى بمزيد من الاهتمام.

互联网在云端。

不，Daniel Voelsen 写道：互联网依赖于复杂的全球基础设施。除了软件标准和网络协议的逻辑层之外，该基础设施还包括物理组件，例如海底电缆和数据中心。这个物理层不可避免地将互联网与各领土国家联系起来，因此应该受到更多关注。

Internet est dans le cloud.

Non, écrit Daniel Voelsen: Internet dépend d‘une infrastructure mondiale complexe. Outre la couche logique des normes et protocoles logiciels, cette infrastructure inclut des composants physiques, tels que des câbles sous-marins et des centres de données (data-centers). Cette couche physique lie inévitablement Internet au monde des états territoriaux, on doit donc y porter une plus grande attention.

Интернет хранится на облаке.

Это не так, говорит Даниэль Воелсен: Интернет зависит от комплексной всемирной инфраструктуры. Кроме логического уровня стандартов и протоколов программного обеспечения, эта инфраструктура включает в себя физические компоненты, такие как подводные кабели и центры обработки данных. Этот физический уровень неизбежно связывает Интернет с миром государств территориальной юрисдикции, поэтому ему следует уделять больше внимания.

El internet está en las nubes.

No, dice Daniel Voelsen: el internet se apoya en una infraestructura global compleja. Más allá del ámbito logístico de estándares de software y protocolos, la infraestructura incluye también componentes físicos, tales como cables submarinos y centros de datos. El ámbito físico inevitablemente ata al internet al mundo de los Estados territoriales y, por lo tanto, debería recibir más atención.

MYTH #38

Robin Tim Weis

The Domain Name System guarantees a global Internet.

Myth: The Internet was devised as universal and global in nature. The Domain Name System as the Internet‘s phone book and the multiple root servers underlying it ensured that everyone will reach every site they want whenever they feel like it. This built-in decentralized resilience will last forever.

Busted: The TCP/IP infrastructure is a pipe dream of the past, as countries are moving forward with new setups that utilize novel ways to circumvent the DNS. In effect, the Internet is being copied and contained in national content silos. The most recent uprooting of the global DNS is underway in Russia. In its recent efforts, the Russian government is actively seeking to replicate the current DNS setup by creating a "system of backup DNS root name servers, independent of the control of ICANN, IANA and VeriSign", as explained in the recently adopted "sovereign Internet" bill. Saudi Arabia has emulated these "sovereign" efforts, restricting DNS outright: DNS request traffic is instead routed through Saudi nationally controlled proxy services. This recent nationalization of the Internet runs contrary to the early international efforts by organizations such as CSNET or the Internet Architecture Board (IAB) that was created in 1983 to guide the evolution of the TCP/IP Protocol Suite and to provide research advice to the burgeoning Internet community.

Given its founding ethos, the Internet's protocols were openly available, and because it's a network of interconnected networks, it's entirely possible to re-create a different network of interconnected networks. Authoritarian nation states are seemingly interested to strip themselves of what some view and communicate as the "western" DNS, looking to create an entirely alternate reality for the majority of their Internet users. Tomorrow's Internet users could see countries vanish from the Internet, if certain governments decide to ban national domains from their own national root servers. The "Splinternet" is born.

Truth: Despite its infrastructure being conceived as global, we slowly enter an age of many national, fragmented Internets. Governments around the world are eager to go live with their "Splinternet." Users no longer should expect to be able to reach all websites. The open nature of DNS is being disassembled as we speak.

Source

William Lehr et al., "Whither the Public Internet?," Journal of Information Policy 9 (2019): 1–42, https://doi.org/10.5325/jinfopoli.9.2019.0001; Charlotte Jee, "Russia Wants to Cut Itself off from the Global Internet. Here's What That Really Means.," MIT Technology Review, 21 March 2019, https://www.technologyreview.com/s/613138/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means.

MYTH #38

Das Domain Name System garantiert ein globales Internet.

Nein, sagt Robin Tim Weis: Auch wenn die Infrastruktur des Internets global konzipiert ist, sehen wir uns allmählich am Beginn eines Zeitalters vieler nationaler, fragmentierter Internets. Auf der ganzen Welt können es Regierungen nicht erwarten, mit ihrem „Splinternet“ online zu gehen. Die Nutzer*innen können nicht davon ausgehen, stets alle Websites erreichen zu können. Die offene Natur des DNS wird auch jetzt, in diesem Augenblick, untergraben.

نظام أسماء المجالات يضمن إنترنت عالمية.

كلا، هكذا يقول روبن تيم فايس: ومع أن بنيتها التحتية تعتبر عالمية، فقد بدأنا ندخل ببطء عصرًا يشمل الكثير من «الإنترنتات» الوطنية المفتتة. فالحكومات حول العالم كلٌّ حريصة على تشغيل شبكة «Splinternet» خاصة بها. وما عاد بإمكان المستخدمين توقُّع الوصول إلى جميع مواقع الويب. فالطبيعة المفتوحة لنظام أسماء المجالات يجري تفكيكها بشكل حثيث حالياً.

域名系统为全球互联网提供保障。

不，Robin Tim Weis 写道：尽管其基础设施被视为全球通用，但我们正逐渐进入多国、分散的互联网时代。世界各地的政府都渴望有自己的“分割网”。用户不再希望能够访问所有网站。正如我们所言，域名解析系统的开放性正在被废除。

Le système de nom de domaine (DNS) garantit un Internet global.

Non, écrit Robin Tim Weis: bien que son infrastructure ait été conçue comme globale, nous entrons lentement dans l’ère d‘un Internet fait de nombreux réseaux nationaux fragmentés. Les gouvernements du monde entier n‘ont qu‘une hâte, lancer leur « Splinternet ». Les utilisateurs ne doivent plus s‘attendre à pouvoir accéder à tous les sites Web. La nature ouverte du DNS est en train d‘être démontée au moment où nous parlons.

Система доменных имен обеспечивает глобальный Интернет.

Это не так, говорит Робин Тим Вайс: Несмотря на то, что инфраструктура была задумана как глобальная, мы медленно вступаем в эпоху множества национальных, раздробленных интернетов. Правительства всего мира стремятся запустить свой «Сплинтернет». Пользователям больше не следует ожидать возможности получить доступ ко всем веб-сайтам. Уже сейчас открытая природа системы доменных имен демонтируется.

El sistema de nombres de dominio garantiza un internet global.

No, dice Robin Tim Weis: a pesar de que su infraestructura es concebida como algo global, hoy en día entramos lentamente en una era de muchos “internets” nacionales y fragmentados. Los gobiernos del mundo están ansiosos por irse a vivir con sus propios “splinternets” (internets fragmentados o “balcanizados”). Los usuarios deberán contar con que ya no podrán tener acceso a todos los sitios web. El desmantelamiento de la naturaleza abierta del sistema de nombres de dominio está ocurriendo en este preciso momento.

MYTH #39

Bernadette Califano and Mariano Zukerfeld

Net Neutrality is secured across the Internet.

Myth: Net neutrality rules prohibit discriminatory practices on the Internet and thus ensure an equal treatment for all packages of information independent of user, content, platform, place or application. Promoting freedom of expression, competition and information exchange on the Internet, net neutrality laws prevent unfair treatment of Internet users.

Busted: Equal treatment of packages independent of user, content, platform etc. rarely exists in practice, even in countries where net neutrality laws are enforced, and particularly in countries located in the Global South. Five empirical situations demonstrate this statement: Traffic management measures carried out by ISPs imply the prioritization of certain data packages over others. The lack of transparency regarding these measures suggest that they are driven by economic aims as opposed to strict technical reasons.

Some powerful content or service providers use content distribution networks (CDNs) or subscribe peering agreements to improve the transit of their contents. Thus, actors who can pay for it, receive an extra boost that speed up the distribution of their contents vis a vis other –smaller – content and services providers.

Net neutrality as a principle applied to signal transport does not prevent discrimination that takes place on higher layers of the OSI model, for instance through search engines ranking. Consequently, some information packages – and users that send and might receive them – are deprioritized. Lack of transparency of algorithms and the absence of “search neutrality” conspire against fair treatment of all Internet users when it comes to content filtering and ranking on platforms.

Differences in terms of bandwidth between countries generate a discrimination against packages coming from peripheral nations. World average download speed was 45 Mbps in 2018. In Sweden it was 94 MBps, and in the United Sates 92 Mbps whereas in Latin America the average was 19 Mbps and in Africa 14 Mbps.

Differences between upload and download speeds involve traffic prioritization of some data packages over others. By large, in most of the world upload speed is much slower than download speed (45 and 22 Mbps respectively). This means that becoming a producer is harder than being a consumer almost everywhere. Certainly, this situation is worsened when the previous point is considered: packages from producers located in peripheral countries are discriminated although net neutrality rules are enforced.

There are thus obvious macro-economic reasons for users of lower purchasing power to be treated unfairly, even when network neutrality laws are in place. This is rarely addressed by proponents of the approach.

Truth: Net neutrality laws can indeed prevent transport-related discrimination, but this benefits large-scale providers of content and services rather than leveling the playing field for users and producers located in “peripheral” countries, as their packages of information suffer from different forms of deprioritization on the Internet. Net neutrality approaches alone are therefore not enough to ensure equality of treatment for users and content from countries with lower levels of Internet access.

■ ***Source***

Mariano Zukerfeld and Bernadette Califano, Discutiendo la neutralidad de la red. De los discursos dominantes a las prácticas en contextos periféricos, 8 Commons (2019) 1, 5-43; Martin Cave and Pietro Crocioni, Does Europe Need Network Neutrality Rules?, 1 International Journal of Communication (2007), 669–679.

MYTH #39

Netzneutralität verhindert Diskriminierung im gesamten Internet.

Nein, sagen Bernadette Califano und Mariano Zukerfeld: Gesetze zur Netzneutralität können durchaus transportbezogene Diskriminierung verhindern, jedoch nützt dies eher Großanbieter*innen von Inhalten und Diensten, statt gleiche Ausgangsbedingungen für Nutzer*innen und Anbieter*innen aus „peripheren“ Ländern zu fördern, da ihre Informationspakete unterschiedlichen Formen von Entpriorisierung im Internet ausgesetzt sind. Konzepte der Netzneutralität allein reichen daher nicht aus, um die Gleichbehandlung von Nutzer*innen und Inhalten aus Ländern mit geringerem Internetzugang zu gewährleisten.

حياد الشبكة يمنع التمييز غير العادل عبر الإنترنت.

كلا، هكذا تقول برناديت كاليفانو وماريانو زوكرفيلد: يمكن لقوانين حياد الشبكة بالفعل منع التمييز المتعلق بالنقل، لكن هذا يعود بالنفع على مقدمي المحتوى والخدمات الكبار دون ضمان تكافؤ الفرص للمستخدمين والمنتجين الموجودين في البلدان «الطرفية»، حيث تعاني حزم المعلومات من أشكال مختلفة من تقليل مستوى الأولوية على الإنترنت. وبالتالي فنُهُج حياد الشبكة وحدها ليست كافية لضمان المساواة في المعاملة للمستخدمين والمحتوى من البلدان التي تتدنى فيها مستويات الوصول إلى الإنترنت.

网络中立防止互联网间的不公平歧视。

不，Bernadette Califano 和 Mariano Zukerfeld 写道：网络中立法律确实可以防止与运输有关的歧视，但这有利于内容和服务的大型供应者，而不是为位于“外围”国家的用户和生产者提供公平的竞争环境，因为他们的信息包在互联网上受到不同形式的去优先次序。因此，仅网络中立方法不足以确保互联网接入水平较低国家的用户和内容的待遇平等。

La neutralité du Net empêche toute discrimination injuste sur Internet.

Non, écrivent Bernadette Califano et Mariano Zukerfeld: les lois sur la neutralité du net peuvent certes empêcher la discrimination liée aux transports, mais cela profite aux grands fournisseurs de contenus et de services et ne nivelle pas le terrain de jeu des utilisateurs et des producteurs situés dans les pays « périphériques », car leurs paquets d‘informations souffrent de différentes formes de dépriorisation sur Internet. Les approches de la neutralité d‘Internet ne suffisent donc pas à elles seules à garantir l‘égalité de traitement des utilisateurs et des contenus provenant de pays où l‘accès à Internet est moins développé.

Сетевой нейтралитет не допускает дискриминацию в Интернете.

Это не так, говорят Бернадетт Калифано и Мариано Цукерфельд: Законодательство о сетевом нейтралитете действительно может не допустить транспортную дискриминацию, но это выгодно скорее крупным поставщикам контента и услуг, и не выравнивает поле для пользователей и поставщиков, расположенных в «периферийных» странах, поскольку их пакеты информации страдают от различных форм деприоритизации в Интернете. Поэтому одних лишь подходов сетевого нейтралитета недостаточно для обеспечения равного режима для пользователей и контента из стран с более низким уровнем доступа в Интернет.

La neutralidad de la red previene discriminaciones injustas a lo largo del internet.

No, dicen Bernadette Califano y Mariano Zukerfeld: las leyes de neutralidad de la red en efecto pueden prevenir discriminaciones relativas al transporte, pero esto beneficia más a los proveedores de contenido y servicios de gran escala más que nivelar el campo de acción con respecto a usuarios y productores localizados en países “periféricos”, ya que sus paquetes de información sufren diferentes formas de despriorización en el internet. Los enfoques de neutralidad de la red por sí mismos no son suficientes para asegurar una igualdad de trato para usuarios y contenidos de países con niveles de acceso al internet más bajos.

MYTH #40

Alina Wernick

The Internet democratizes innovation.

Myth: Anyone, anywhere can become an innovator because the Internet provides us with an unprecedented amount of knowledge and tools to create innovations. The locus of innovation will shift from companies to people. Thanks to the Internet access to innovations becomes more equal on a global scale.

Busted: The knowledge, information and data relevant for fueling innovative activity is not always available online due to a lack of incentives to share them, legal constraints or both. These resources may be behind a paywall, protected as personal data or as intellectual property. Not all innovators are willing to share their innovations online, as this may undermine their business model. Innovations that are risky and require high investments in research and development are unlikely to be executed online instead of corporate environment. IP rights such as patents encourage such innovative activity by protecting innovators from free-riding. However, they constrain the use and reuse of such innovations online.

There are, nevertheless, both individuals and communities of innovators who actively share and create innovations online. A famous example is open source software development, where IP rights are harnessed to enable collaborative software development. (→ #9) Indeed, the Internet enables democratic access to and co-creation of innovations that can be designed and developed in modules, when collaborators are non-competitors, collaborative development enhances the quality of the innovation and where the innovation itself can be implemented in a digital form (Baldwin and von Hippel, 2011). However, the availability of Internet connection is not enough to foster online innovation activity. The level of trust present in society influences the intensity of engagement in open source software development, explaining the differences in online creation between cities with otherwise similar technological conditions and levels of prosperity (Stephany et al. 2019).

Finally, the Internet is also a limited medium for disseminating innovations that take a tangible form. The design of an innovative object may be shared over the Internet, but the object itself must be manufactured. As a consequence, mass production that harnesses the economies of scale remains in many situations the most effective means to democratize access to tangible, innovative products. (vgl. Baldwin and von Hippel, 2011). While 3D printing technology does enable on-demand manufacturing of designs uploaded from the Internet (something the "maker community" makes use of), the variety of designs available and the complexity of products that can be 3D printed are limited.

Truth: The Internet facilitates co-creation of modular, digitally implementable innovations, such as open source software. However, incentive structures, as well as legal and societal factors constrain the participation of "everyone" in innovation communities and the sharing of innovations online. The majority of tangible, risky or costly innovations will continue to being produced from within companies.

Source

Carliss Baldwin and Eric Von Hippel, Modeling a paradigm shift: From producer innovation to user and open collaborative innovation, Organization Science 22 (2011), 1399-1417; Fabian Stephany, Fabian Braesemann and Mark Graham, Coding Together - Coding Alone: The Role of Trust in Collaborative Programming, SocArxiv (2019) https://osf.io/preprints/socarxiv/8rf2h/download .

MYTH #40

Das Internet demokratisiert Innovation.

Nein, sagt Alina Wernick: Das Internet ermöglicht im Netz die Mitgestaltung modularer, digital realisierbarer Innovationen wie beispielsweise Open-Source-Software. Anreize für Innovationen sowie rechtliche und gesellschaftliche Faktoren schränken die Teilnahme an demokratischen Innovations-Communitys und den Austausch von Innovationen im Internet ein. Die Mehrzahl der greifbaren, risikoreichen oder kostenintensiven Innovationen wird auch künftig von Unternehmen produziert werden.

الإنترنت تضفي الطابع الديموقراطي على الابتكار.

كلا، هكذا تقول ألينا فيرنيك: تتيح الإنترنت المشاركة على الشبكة في إنشاء ابتكارات نمطية قابلة للتنفيذ رقميًّا كالبرامج مفتوحة المصدر. تحدّ حوافز المبتكرين والعوامل القانونية والمجتمعية من حجم المشاركة في مجتمعات الابتكار الديمقراطية وتشارُك الابتكارات عبر الإنترنت. وسيبقى إنتاج غالبية الابتكارات الملموسة أو المحفوفة بالمخاطر أو باهظة التكلفة محصوراً بالشركات.

互联网使创新民主化。

不，Alina Wernick 写道：互联网使得模块在线共建和可执行的数字化创新成为可能，例如开源软件。创新者的动机以及法律和社会因素限制了参与民主创新社区的参与以及共享网络创新。大多数有形、高风险或成本高昂的创新仍将由公司负责进行。

Internet démocratise l‘innovation.

Non, écrit Alina Wernick: Internet permet la co-création en ligne d’innovations modulaires pouvant être mises en œuvre numériquement, telles que les logiciels open source. Les motivations des innovateurs ainsi que les facteurs juridiques et sociaux limitent la participation aux communautés d‘innovation et le partage de ces innovations en ligne. La majorité des innovations tangibles, risquées ou coûteuses resteront produites par les entreprises.

Интернет демократизирует инновации.

Это не так, говорит Алина Верник: Интернет позволяет совместно создавать онлайн такие модульные инновации, как программное обеспечение с открытым исходным кодом, реализуемое в цифровом виде. Заинтересованность новаторов, наравне с правовыми и социальными факторами сдерживают участие в демократических инновационных сообществах и распространение инноваций в Интернете. Большая часть материальных, рискованных или дорогостоящих инноваций так и будут производиться компаниями.

El internet democratiza la innovación.

No, dice Alina Wernick: el internet permite la cocreación online de innovaciones modulares y digitalmente implementables, tales como el software de código abierto. Los incentivos de los innovadores, así como factores legales y sociales, restringen la participación en comunidades de innovación democrática y el intercambio de innovaciones en el internet. La mayoría de las innovaciones tangibles, arriesgadas o costosas seguirá siendo producida por compañías.

MYTH #41

Paul Belleflamme

Network effects cannot be overcome.

Myth: Positive network effects arise when the value of a solution (product, service, platform) improves as more users adopt it. As early adoptions enhance future adoptions, a solution that manages to get ahead of the alternative ones will eventually - and irreversibly - dominate.

Busted: Network effects arise if users care about participation and usage decisions of other users when taking their own decision. If users belong to a unique group, network effects are "direct", as more usage within the group directly affects each group member (as with communication devices). Network effects can also arise across users of distinct groups, as is the case on many digital platforms (Airbnb becomes more attractive for guests by having more hosts on board, and vice versa); here, network effects are indirect: an additional user affects the other users in her group not directly but via the increased participation in the other group.

In the presence of positive (direct or indirect) network effects, more usage enhances value, which triggers more usage, and so on. This self-reinforcing process is conducive to winner-takes-all situations (a unique solution eventually attracts most - if not all - users), followed by a form of lock-in (users are not willing to switch on their own because alternative solutions only become attractive in the unlikely event that all users switch together). Yet, a number of countervailing forces may curb the snowballing power of positive network effects. First, network effects are rarely positive all over: they may be restricted to small groups of users (such as pre-existing friends on a social media), or negative within some group (like competing sellers on a trading platform), or become negative at some point (because the network infrastructure gets congested). Second, differentiation can play strongly against network effects: several solutions may coexist because they cater to the specific needs of different segments of users (like rival game consoles); also, a new and improved solution may displace a dominant one because it provides users with a sufficiently large value to overcome the lock-in (think of Facebook displacing MySpace).

So, even if winner-takes-all situations do exist (think of the current 95% market share of Google search engine in Europe), they cannot be explained solely by the presence of positive network effects: supply-side economies of scale or scope also contribute to their emergence, while anticompetitive conducts may play a part in their persistence.

Truth: Positive network effects generate self-reinforcing processes that may lead to winner-takes-all situations. Yet, there exist countervailing forces that makes it possible for solutions to coexist, and for once dominating solutions to be overcome by new, improved, ones.

Source

Paul Belleflamme and Martin Peitz, Platform and Network Effects, in Luis C. Corchon and Marco A. Marini (eds), Handbook of Game Theory and Industrial Organization (Cheltenham: Edward Elgar, 2018), https://ssrn.com/abstract=2894906; Andrei Hagiu and Simon Rothman, Network Effects Aren't Enough, Harvard Business Review (April 2016), https://hbr.org/2016/04/network-effects-arent-enough.

MYTH #41

Netzwerkeffekte sind unüberwindbar.

Nein, sagt Paul Belleflamme: Positive Netzwerkeffekte erzeugen sich selbst verstärkende Prozesse, die dazu führen können, dass der Stärkste letztlich alles bekommt. Gleichwohl existieren auch Gegenkräfte zu Netzwerkeffekten, die parallele Angebote oder konkurrierende Unternehmen möglich machen und durchaus dazu führen können, dass einmal vorherrschende Lösungen durch neue, bessere ersetzt werden.

ا يمكن التغلب على تأثيرات الشبكة.

كلا، هكذا يقول بول بيلفلام: تولد تأثيرات الشبكة الإيجابية عمليات ذاتية الدعم قد تؤدي إلى مواقف يأخذ فيها الفائز كل شيء. ومع ذلك توجد قوى متضادة تتيح للحلول أن تتواجد جنبًا إلى جنب وتتيح للحلول الجديدة المحسّنة التغلب على الحلول التي هيمنت ذات يوم.

网络效应无法克服。

不，Paul Belleflamme 写道：积极的网络效应产生自我强化的过程，可能会出现赢家通吃的情况。但是，存在使解决方案共存成为可能的对抗力，并且曾经占据主导地位的解决方案将被新的、改进的解决方案取代。

Les effets de réseau ne peuvent pas être évités.

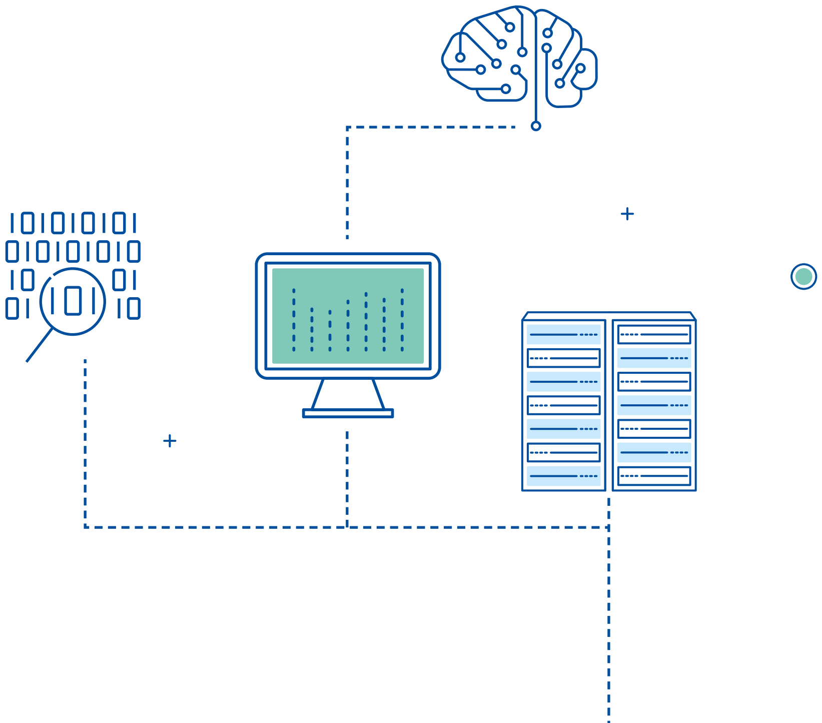
Non, écrit Paul Belleflamme: les effets de réseau positifs génèrent des processus qui s’auto-renforcent et peuvent conduire à des situations où tout va au vainqueur. Cependant, il existe des forces compensatrices qui permettent la coexistence de solutions et qui, pour une fois, permettent aux solutions dominantes d‘être surpassées par de nouvelles solutions améliorées.

Сетевые эффекты нельзя преодолеть.

Это не так, говорит Пол Бельфламм: Положительные сетевые эффекты формируют взаимодополняющие процессы, которые могут привести к ситуациям, где «победитель получает все». Тем не менее, существуют уравновешивающие силы, позволяющие решениям сосуществовать, и заменять доминирующие решения новыми, улучшенными.

Los efectos de red no pueden ser superados.

No, dice Paul Belleflamme: los efectos de red positivos generan procesos que se autorrefuerzan y que podrían llevar a situaciones de tipo “el ganador se lo lleva todo”. Sin embargo, existen fuerzas compensatorias que hacen posible la coexistencia de soluciones y que soluciones que alguna vez fueron dominantes sean superadas por otras nuevas y mejores.



CHAPTER 5

Data and disruption

Daten und Disruption

الإدماج والتكامل

数据与中断

Données et perturbations

Данные и сбои

Datos y disrupción

MYTH
#42

Matthias Spielkamp

Algorithms are always neutral.

Myth: Because an algorithm is nothing but a set of instructions that is applied to data – that usually comes in the form of numbers – it can contain no bias or prejudice that would have an influence on the outcome produced by using the algorithm.

Busted: Algorithms are designed by humans; so are algorithmic decision-making systems – from network management that favours certain forms of content over others (net neutrality) to “AI” that is supposed to automatically distinguish hate speech, disinformation or terrorist propaganda from journalism, parody and other forms of legitimate content. (→ #18; → #43) All of these systems use value judgments to arrive at their results: To perform its task, an algorithm needs to “know” what data package to treat differently from others, what criteria define a certain mode of expression. Leaving the question aside whether algorithms will ever be able to assess speech correctly (they will not), it is obvious that such definitions are always developed by human beings with certain intentions. We would not qualify these definitions as neutral, and neither is the algorithm that acts on their basis.

A benevolent reading of the myth is that algorithms subject all inputs to the same set of instructions and therefore act indiscriminately, and that they do not have any intentions of their own. This is true, but obviously beside the point.

With regard to so-called machine-learning techniques, another aspect comes into play. When algorithms are trained by feeding them with large data sets in order for them to identify patterns and “learn” from them (so-called “training data”), then it needs to be understood that these data sets usually contain biases that are inherent in human society. If a self-learning system draws conclusions on the basis of biased data, these conclusions will generally be biased, too, and therefore not neutral.

Truth: Algorithms are either directly designed by humans or, if self-learning, develop their logic on the basis of human-controlled and -designed processes. They are neither “objective” nor “neutral” but outcomes of human deliberation and power struggles.

Source
Aylin Caliskan Islam, Joanna J. Bryson, Arvind Narayanan: Semantics derived automatically from language corpora necessarily contain human biases, Computing Research Repository (2017), https://arxiv.org/abs/1608.07187; Alex Salkever, Vivek Wadhwa: A.I. Bias Isn’t the Problem. Our Society Is (2019), https://fortune.com/2019/04/14/ai-artificial-intelligence-bias.

MYTH
#42

Algorithmen sind immer neutral.

Nein, sagt Matthias Spielkamp: Algorithmen werden entweder direkt von Menschen entwickelt oder entwickeln ihre Logik beim Selbstlernen auf der Grundlage von vom Menschen gesteuerten und gestalteten Prozessen. Sie sind weder „objektiv“ noch „neutral“, sondern das Ergebnis menschlicher Überlegungen und Machtinteressen.

الخوارزميات محايدة دائمًا

كلا، هكذا يقول ماتياس شبيلكامب: الخوارزميات نوعان: نوع يصممه الإنسان مباشرة، وخوارزميات التعلم
الذاتي التي تطور منطقها على أساس عمليات يتحكم فيها ويصممها الإنسان. وهي ليست «موضوعية» ولا
«محايدة» بل نتاج المداولات البشرية والصراعات على السلطة.

算法始终中立

不，Matthias Spielkamp 写道：算法直接由人进行设计，或在自学的情况下，在人为控制和设计过程的基础上发展其逻辑。它们既非“客观”亦非“中立”，而是人类商议和权力斗争的结果。

Les algorithmes sont toujours neutres

Non, écrit Matthias Spielkamp: les algorithmes sont conçus directement par les humains ou développent leur logique sur la base de processus conçus et contrôlés par l’homme. Ils ne sont ni « objectifs », ni « neutres », mais résultent de délibérations humaines et de luttes de pouvoir.

Алгоритмы всегда нейтральны

Это не так, говорит Матиас Спилкамп: Алгоритмы либо разрабатываются непосредственно людьми, либо, если они самообучаемые, совершенствуют свою логику на основе контролируемых и разработанных человеком процессов. Не будучи ни «объективными», ни «нейтральными», они являются результатом человеческих обдумываний и борьбы за власть.

Los algoritmos siempre son neutrales.

No, dice Matthias Spielkamp: los algoritmos han sido diseñados directamente por humanos o, si poseen capacidad de autoaprendizaje, desarrollan su lógica en base a procesos diseñados y controlados por humanos. No son ni “objetivos” ni “neutrales”, sino el resultado de la deliberación y las luchas de poder humanas.

MYTH #43

Christian Katzenbach

AI will fix it.

Myth: “Artificial intelligence” (AI) is the key technological development of our time. AI will not only change how we live, communicate, work and travel tomorrow, AI-based solutions will fix the fundamental problems of our societies from the detection of illnesses and misinformation to online hate speech and urban mobility.

Busted: The current hype about AI is strongly connected to the myth that AI will by itself solve key problems of our societies. In the 2018 US congressional hearings, Facebook’s CEO Marc Zuckerberg used phrases such as “AI will fix this” and “in the future we will have technology that addresses these issues” more than a dozen times when pressed upon issues of misinformation, hate speech and privacy. In other sectors, businesses and technologists promise that AI-powered technologies and products will detect cancer in early stages, identify tax fraud patterns, guide vehicles efficiently through urban areas and identify antisocial and criminal behaviour in public spaces.

The narrative that technology will fix social problems is a recurrent theme in the history of technology and society. The “technological fix” (Rudi Volti) seeks functional solutions for problems that are social and political in nature: Autonomous vehicles might drive more safely through the city (by some criteria), but will not provide urban mobility to broad segments of the population. Filtering software might get better by identifying misinformation and hate speech, but will not eradicate it and will always be unable to strike the perfect (and widely accepted) balance between freedom of expression and harmful speech. These problems are fundamentally social in nature, so there is not that one single right answer that can be technologically implemented.

Talk about “AI fixing things” is also misleading because it obfuscates the human labour and the social relations that the seemingly autonomously operating technologies are building upon. AI-based products don’t just appear, they are man-made. (→ #18; → #42) Typical AI-powered devices and services such as autonomous vehicles and image detection solutions are products of companies with commercial interests and normative assumptions – and these are inscribed into the products itself. What is more, AI products are the results of immense amounts of human labour, ranging from developing complex mathematical models to mundane activities such as training image recognition AIs picture by picture.

Consequently, even if AI-powered services and devices perform perfectly functional according to preset criteria in the future, the phrase “AI will fix this” will still be utterly misleading. Many of these problems are fundamentally social in nature and do not yield a functional solution. AI technology is not an autonomous agent but constructed by humans and society.

Truth: While AI cannot fix everything, humans using AI might fix some things. Rapid developments in AI technologies provide opportunities for many stakeholders to be more responsive to societal challenges. These technologies will contribute to innovations across many societal sectors and change the way we live, communicate, work and travel – not automatically for the public good, though.

Source

Evgeny Morozov, To save everything, click here: The folly of technological solutionism (New York: PublicAffairs, 2013); Julia Powles and Helen Nissenbaum, The Seductive Diversion of ‘Solving’ Bias in Artificial Intelligence, Medium, 8 December 2018, https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53.

MYTH #43

Künstliche Intelligenz wird es schon richten.

Nein, sagt Christian Katzenbach: Zwar kann die KI nicht alles richten, jedoch besteht durchaus die Chance, dass Menschen mithilfe der KI einige Dinge in Ordnung bringen. Die rasante Entwicklung von KI-Technologien bietet vielen Stakeholdern die Möglichkeit, besser auf gesellschaftliche Herausforderungen zu reagieren. Diese Technologien können in vielen gesellschaftlichen Bereichen Innovationen fördern und die Art und Weise verändern, wie wir leben, kommunizieren, arbeiten und reisen – allerdings nicht automatisch zum Wohle der Allgemeinheit.

الذكاء الاصطناعي سيصلح كل شيء.

كلا، هكذا يقول كريستيان كاتزنباخ: على الرغم من أن الذكاء الاصطناعي لا يمكنه إصلاح كل شيء، إلا أن البشر الذين يستخدمون الذكاء الاصطناعي ربما يصلحون بعض الأشياء. وتتيح التطورات السريعة في تكنولوجيات الذكاء الاصطناعي فرصًا للكثير من أصحاب المصلحة ليكونوا أكثر استجابة للتحديات المجتمعية. ستساهم هذه التكنولوجيات في الابتكارات عبر الكثير من القطاعات المجتمعية وتُغيّر الطريقة التي نعيش بها ونتواصل ونعمل ونسافر، لكن ذلك لن يكون بشكل تلقائي في سبيل الصالح العام.

人工智能会解决一切问题。

不，Christian Katzenbach 写道：虽然人类借助人工智能可解决一些问题，但人工智能无法解决所有问题。人工智能技术的快速发展为很多利益相关方提供了更好应对社会挑战的机会。这些技术将为很多社会领域的创新做出贡献，并改变我们的生活、交流、工作和旅行方式——但不是为了公共利益而自动改变。

L‘IA va réparer ça.

Non, écrit Christian Katzenbach: l‘IA ne pouvant pas tout réparer, les humains utilisant l‘IA pourront réparer certaines choses. Les développements rapides des technologies de l‘IA offrent des opportunités d‘être plus réactifs aux défis sociétaux à de nombreux acteurs. Ces technologies contribueront aux innovations dans de nombreux secteurs de la société et changeront notre façon de vivre, de communiquer, de travailler et de voyager, mais pas automatiquement pour le bien public cependant.

ИИ все исправит.

Это не так, говорит Кристиан Катценбах: ИИ не может исправить все, тогда как человек, использующий его может нечто исправить. Стремительное развитие технологий искусственного интеллекта дает возможность многим заинтересованным участникам более оперативно реагировать на социальные вызовы. Эти технологии будут благоприятствовать инновациям во многих общественных секторах и изменят наш образ жизни, общение, работу и путешествия во имя общего блага, хотя все же не автоматически.

La inteligencia artificial lo arreglará todo.

No, dice Christian Katzenbach: mientras que la inteligencia artificial no puede arreglarlo todo, los humanos que utilizan la inteligencia artificial podrían arreglar algunas cosas. El rápido desarrollo de las tecnologías de inteligencia artificial brinda oportunidades a muchos actores de prestar más atención a los problemas sociales. Estas tecnologías darán aportes a innovaciones en muchos sectores de la sociedad y cambiarán la forma en que vivimos, nos comunicamos, trabajamos y viajamos. Sin embargo, no automáticamente para el bien público.

MYTH #44

Philippe Lorenz and Kate Saslow

The future of AI is in the hands of companies.

Myth: National governments are unable to strengthen their own AI innovation base. Private companies buy up national AI resources. States are unable to develop middle- to long-term policy plans regarding strong national AI approaches because policy makers don't fully understand what AI actually is or means.

Busted: AI technology differs from previous emerging technologies because private sector companies are now innovators in AI technologies. But states can still influence the creation of AI ecosystems where such innovative firms will thrive. This requires providing companies and universities with the necessary resources to produce cutting-edge AI technologies. Private sector actors and state actors merely pursue different roles.

AI is no magic: The industry inputs necessary to produce machine learning (ML) technologies are data, software, hardware, and talent. (→ #43). Understanding ML as a composition of these inputs allows policy makers to grasp its economic relevance and recognize the significance of actors who produce and apply this technology. But the rhetoric around AI in policy today remains inconsistent and vague. A deeper understanding of AI is urgently needed. It will improve the debate among the foreign policy community and thus provide the basis for better monitoring of global trends, which can inform policy making at home.

In the AI field, companies matter, as innovation around ML disproportionately stems from private sector entities. Companies to watch focus their research and development efforts on creating specific core ML products, and have a revenue stream based on ML driven applications. Such are true "AI companies" and they push the development and adoption of AI technologies.

But this does not mean that states have no role to play: Foreign service officers are instrumental in gathering and analyzing political and economic matters with regional expertise and then reporting this information back to the government headquarters. The pace of AI development and deployment is fast; its economic importance substantial. But resources to actively monitor global developments are currently limited. However, policy makers around the world have begun to understand the importance of AI and assert themselves into the debate. This is reflected by numerous international initiatives and fora devoted to AI governance.

But these fora and initiatives lack teeth and governments still lack a common nomenclature to discuss and monitor global developments in AI. Leveraging the international network of embassies and the strength of foreign services – information gathering and analysis – foreign services can significantly help government headquarters shape foreign and domestic policy around AI. This can help raise awareness and capacity for more comprehensive and more effective policy making for AI governance. States thus play an important role by providing an ecosystem conducive to AI innovation, and by tracking strategic developments in AI innovation globally.

Truth: States continue to play an essential role in governing AI. But they must be proactive to know what to do. Policymakers today must consider how states can influence industry inputs necessary to create machine learning technologies (data, software, hardware, and talent) and provide governments with a clear perspective on how to defend and enhance their strategic development of AI ecosystems.

Source

Philippe Lorenz and Kate Saslow, Demystifying AI & AI Companies. What foreign policy makers need to know about the global AI industry (July 2019), Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/demystifying_ai_and_ai_companies.pdf.

MYTH
#44

Die Zukunft der Künstlichen Intelligenz liegt in den Händen von Unternehmen.

Nein, sagen Philippe Lorenz und Kate Saslow: Die Staaten spielen nach wie vor eine wesentliche Rolle bei der Regulierung von „Künstlicher Intelligenz“, müssen jedoch proaktiv handeln, um sinnvoll politische Gestaltungsräume nutzen zu können. Die Politik wiederum muss umfassend Daten sammeln und den Regierungen eine klare Perspektive bieten, wie sie die strategische Entwicklung von KI-Ökosystemen verteidigen und verbessern können.

مستقبل الذكاء الاصطناعي في أيدي الشركات.

كلا، هكذا يقول فيليب لورينتس وكيت ساسلو: ما زالت الدول تلعب دورًا أساسيًّا في إدارة الذكاء الاصطناعي، لكن يجب أن تكون استباقية لمعرفة ما عليها فعله. يجب على صانعي السياسات اليوم جمع البيانات بطريقة شاملة وتزويد الحكومات بمنظور واضح حول الكيفية التي تدافع بها عن تطويرها الاستراتيجي للنظم الإيكولوجية للذكاء الاصطناعي وتعزّزه.

人工智能的未来掌握在公司手中。

不，Philippe Lorenz 和 Kate Saslow 写道：各国继续在人工智能治理领域发挥重要作用。但它们必须掌握主导权，知道该怎么做。目前的政策制定者必须全面收集数据，并向政府提供有关如何捍卫和加强人工智能生态系统战略性发展的明确看法。

L‘avenir de l‘IA est entre les mains des entreprises.

Non, écrivent Philippe Lorenz et Kate Saslow : les États continuent à jouer un rôle essentiel dans la gouvernance de l‘IA. Mais ils doivent être proactifs pour savoir quoi faire. Les décideurs politiques d‘aujourd‘hui doivent collecter les données de manière exhaustive et donner aux gouvernements une perspective claire sur la manière de défendre et d‘améliorer leur développement stratégique des écosystèmes de l‘IA.

Будущее ИИ зависит от компаний.

Это не так, говорят Филипп Лоренц и Кейт Саслоу: Государства продолжают играть важную роль в контроле за ИИ. Но они должны быть способны думать наперед, чтобы знать, как поступать. Политики сегодня должны тщательно собирать данные, чтобы давать правительствам четкое представление о том, как защищать и улучшать стратегическое развитие экосистем ИИ.

El futuro de la inteligencia artificial está en manos de las compañías.

No, dicen Philippe Lorenz y Kate Saslow: los Estados siguen jugando un papel fundamental en el control de la inteligencia artificial. Pero deben ser proactivos para saber lo que tienen que hacer. Hoy en día, los actores políticos deben recoger datos de forma integral y proporcionar a los gobiernos una perspectiva clara respecto a cómo defender y optimizar el desarrollo estratégico de los ecosistemas de inteligencia artificial.

MYTH #45

Paula Helm with Tobias Dienlin, Johannes Eichenhofer and Katharina Bräunlich

Privacy is dead.

Myth: Privacy is dead. It fell victim to new socio-technical phenomena such as indiscriminate mass surveillance, the collapse of contexts, smartphones, wearables, social media, and the Internet of Things. People, however, don't bother: They use services that are programmed to collect data, share vast amounts of data without reflection, and do not care if the become fully transparent.

Busted: Privacy has been declared dead – not only once, but multiple times. In 1874, The Times published The Abolition of Privacy. In 1909, The Washington Post stated that "only one hiding spot remains in the world. The south pole [...]." In 1999, Scott McNealy (of Sun Microsystems) stated "you already have zero privacy – get over it". In these publications – and many others – privacy was consigned to its grave because of some sweeping societal and technological changes such as the invention of the photo camera, or the Internet. Given this apparent inclination to die and the latest technological developments, privacy surely must be dead as a doornail?

Certainly not. The above mentioned shows primarily one thing: privacy is immortal. Indeed, enabled by the Internet, Big Data technologies and the pervasion of Smartphones and the Internet of Things, privacy is currently being commodified, sold, traded, exploited, neglected, and abandoned. However, to a varying extent that has always been the case. The abolition of privacy was never total. People have constantly found ways to separate themselves from each other, political entities, and corporate companies because they find in privacy a precondition for their individual autonomy, psychological integrity and their ability to build personal relationships.

It has been said that people today willingly give up their privacy – but that is not correct. Numerous empirical studies have shown that people do in fact act in the interest of privacy – also on social media. The more they are concerned about it, the less information they share. When doing so, however, they are confronted with increasingly difficult choices between adhering to powerful imperatives of sharing and connectivity on the one hand and their requirements for privacy on the other.

From a societal perspective, privacy today – probably even more than ever – also functions as a democratic force. When being called upon by political collectives and activists who struggle for their communicative autonomy, privacy is in fact being enacted as a social practice. (→ #14) This practice is crucial for the protection of a vivid democratic culture, where different opinions may co-exist and be deliberated upon. To preserve such culture, more support for Privacy enhancing technologies is needed – for example, anonymous Web browsers such as TOR - which already exist but require to be improved and established as default. (→ #17)

Truth: In some areas and especially for underprivileged people, privacy has become precarious. This is concerning. Privacy should not be turned into a luxury. Reacting to this, privacy currently receives much attention. Both in everyday life and in academia, privacy is indeed enjoying a renaissance as social practice and political value.

Source

Paula Helm, Johannes Eichenhofer, Reflektionen zu einem social turn in den privacy studies. In Martin Hennig et al.: Digitalität und Privatheit (Bielefeld: Transcript, 2019), 139-165; Tobias Dienlin, Miriam Metzger, An extended privacy calculus model for SNSs—Analyzing self-disclosure and self-withdrawal in a representative U.S. sample, Journal of Computer-Mediated Communication, 21 (2016), 368–383, https://doi.org/10.1111/jcc4.12163.

MYTH #45

Die Privatsphäre ist tot.

Nein, sagen Paula Helm, Tobias Dienlin, Johannes Eichenhofer und Katharina Bräunlich: In einigen Bereichen und insbesondere für benachteiligte Menschen ist der Schutz der Privatsphäre kompliziert. Es ist in der Tat bedenklich, wenn die Privatsphäre und die von ihrem Schutz abhängigen Werte wie politische Freiheit, gesellschaftlicher Zusammenhalt und persönliche Autonomie zu Luxusgütern werden. Als Reaktion auf die in letzter Zeit zu beobachtende Prekarität des Privaten wird diesem seit einiger Zeit jedoch wieder große Aufmerksamkeit gewidmet. Sowohl im Alltag als auch in der Wissenschaft erlebt das Private eine Renaissance als gesellschaftliche Praxis und politischer Wert.

الخصوصية لم يعد لها وجود.

كلا، هكذا تقول بولا هيلم وتوبياس دينلين ويوهانس أيشنهوفر وكاترينا براونليش: في بعض المناطق، لا سيما فيما يخص الأشخاص المحرومين، أصبحت الخصوصية شيئًا محفوفًا بالمخاطر. وهذا في الواقع مصدر قلق لأنه يحوّل الخصوصية والقيم الهامة المتمثلة في الحرية السياسية والسلامة الاجتماعية والاستقلالية الشخصية التي تحميها إلى رفاهية. لكن نظرًا لوجودها المحفوف بالمخاطر، تحظى الخصوصية في الوقت الراهن أيضًا باهتمام كبير. ففي كل من الحياة اليومية والأوساط الأكاديمية، تشهد الخصوصية بالفعل انبعاثًا كممارسة اجتماعية وقيمة سياسية.

隐私已死。

不，Paula Helm, Tobias Dienlin, Johannes Eichenhofer 和 Katharina Bräunlich 写道：在某些地区，尤其是贫困地区，隐私已经变得岌岌可危。这确实是一个令人担忧的问题，因为这会将隐私以及隐私保护的政治自由、社会诚信和个人自治的重要价值观转变为奢侈品。但作为对最近隐私不安全现象的回应，目前隐私受到了很多关注。无论是在日常生活中还是在学术界，隐私确实正被视为社会实践和政治价值的复兴。

La confidentialité est morte.

Non, écrivent Paula Helm, Tobias Dienlin, Johannes Eichenhofer et Katharina Bräunlich: dans certaines régions et en particulier pour les personnes défavorisées, la confidentialité est devenue une denrée rare. C'est effectivement un sujet d'inquiétude, car la confidentialité et les valeurs importantes de liberté politique, d'intégrité sociale et d'indépendance individuelle qu'elle protège deviennent un luxe. Mais, en réaction à sa nouvelle rareté, la confidentialité suscite également une grande attention. Tant dans la vie quotidienne que dans le monde universitaire, on assiste à une renaissance de la confidentialité en tant que pratique sociale et valeur politique.

Приватности не существует.

Это не так, говорят Паула Хельм, Тобиас Динлин, Йоханнес Айхенхофер и Катарина Брейнлих: Конфиденциальность стала ненадежной в некоторых сферах, особенно для уязвимых категорий населения. Это действительно проблема, потому что это превращает конфиденциальность и основные ценности, такие как политическая свобода, социальная неприкосновенность и личная автономия, которые она защищает, в роскошь. Но, реагируя на недавнюю ненадежность, конфиденциальности в настоящее время также уделяется много внимания. Как и в повседневной жизни, так и в научных кругах, конфиденциальность действительно переживает возрождение в качестве социальной практики и политической ценности.

La privacidad ha muerto.

No, dicen Paula Helm, Tobias Dienlin, Johannes Eichenhofer y Katharina Bräunlich: en algunas áreas y especialmente para grupos desfavorecidos, la privacidad se ha vuelto precaria. Este es un hecho preocupante pues convierte la privacidad y los valores importantes de libertad política, integridad social y autonomía personal que protege en bienes de lujo. Sin embargo, en reacción a su reciente precariedad, la privacidad actualmente también recibe mucha atención. Tanto en la vida diaria como en el ámbito académico, la privacidad está en efecto disfrutando de un renacimiento como práctica social y valor político.

MYTH #46

Stephan Dreyer

The Internet never forgets.

Myth: Everything that is written, uploaded or shared online will stay online forever. That one photo from your college party will compromise your chance to get the job. The Internet is a giant archive that holds truths and lies forever, with consequences for all our lives and memories.

Busted: Due to its more or less decentralized structure, the marginal costs of digital copies and help by millions and millions of users and local storage devices, many things linger much longer in the Internet, and in our memories. General and specialized search engines enable us to purposefully find a lot of information over a long time. Whole business areas have evolved that offer services like "online reputation management".

The so-called Streisand effect is probably the most famous dilemma in this area: By actively trying to suppress a specific text, picture or video from the Internet one is attracting attention to the attempted content removal and, thus, actually making that very information even more well known. So yes, for any information that at any point in time had gone viral, it will be cumbersome to have this information erased from the Internet forever. But these cases are very special and – compared to the amount of information bits on the Internet – exceedingly rare.

For most content online the prevailing premise is that it will be gone sooner or later: All studies that analyzed the availability of a corpus of online resources showed that there is a high amount of so called "URL rot" or "link rot". Reasons for an online resource to diminish or change are, inter alia, service or server cessation, removal of a second level domain (lately even of a top level domain), account deletion or suspension, content deletion or relocation, changed content, URL shortener decay, redirected links or embedded content decay.

Moreover, the users' approach to self-disclosure and privacy in general has changed quite a bit in the last ten years. The myth already has resulted in more restricted profiles and accounts, for instance on social networks, making public access to unflattering photos from college parties much less common.

And then there is jurisprudence and regulation where anyone is being granted a "right to be forgotten" to have search engine results delisted that infringe their personality rights. (→ #45) The GDPR's right to erasure confirms this approach by granting data subjects the possibility to make a claim aiming at the deletion of personal data on the side of the controller.

Both the decay of resources and the legal instruments to delete specific content on the Internet show that it is not the perennial global information archive many people think. In fact, ordinary content does not show the best pre-conditions for digital preservation at all.

Truth: Many files online show a short half-life period, and significant decay in services and URL rot can be observed. Regulations aiming at deleting information or delisting specific search results reinforce such phenomena. Usual online content is not suited for long-term archiving – and remembering.

Source

Andrew Neville, Is it a Human Right to be Forgotten? Conceptualizing the World View, Santa Clara J. Int'l L. 15 (2017) 157, https://digitalcommons.law.scu.edu/scujil/vol15/iss2/2; Shawn Walker and Sheetal Agarwal, The missing link: a preliminary typology for understanding link decay in social media, IConference Proceedings 2016, http://hdl.handle.net/2142/89413.

MYTH #46

Das Internet vergisst nicht.

Nein, sagt Stephan Dreyer: Viele Dateien im Netz besitzen nur eine kurze Halbwertszeit, und viele Dienste und URLs sind langfristig nicht mehr erreichbar. Verstärkt werden diese Phänomene durch rechtliche Ansprüche auf Datenlöschung oder Auslistung aus bestimmten Suchergebnissen. Weder eignen noch lohnen sich viele Onlineinhalte für eine Langzeitarchivierung.

الإنترنت لا تَنسى أبدًا.

كلا، هكذا يقول شتيفان دراير: يتمتع الكثير من الملفات على الإنترنت بعمر نصفيّ قصير، ويمكن ملاحظة تناقص كبير في الخدمات وفقدان عناوين URL لصلاحيتها. تُعزز اللوائح التنظيمية التي تهدف إلى حذف المعلومات أو إلغاء إدراج نتائج بحث معينة من هذه الظواهر، فالمحتوى المعتاد على الإنترنت غير مناسب للأرشفة والتذكّر على المدى الطويل.

互联网永远不会忘记。

不，Stephan Dreyer 写道：网络上的很多文件都有短暂的半衰期，并且可以观察到服务的显著衰败和 URL 失效。旨在删除信息或除名特定搜索结果的法规强化了这种现象。网络上常见的内容不适合长期存档和记录。

Internet n‘oublie jamais.

Non, écrit Stephan Dreyer : de nombreux fichiers en ligne ont une demi-vie et on peut observer une dégradation significative des services et de l‘URL associés. Les réglementations visant à supprimer des informations ou à supprimer des résultats de recherche spécifiques renforcent ces phénomènes. Le contenu en ligne habituel n‘est pas adapté à l‘archivage à long terme ni à la mémorisation.

Интернет все помнит.

Это не так, говорит Стефан Драйер: У многих файлов в Интернете короткий период полураспада, также можно наблюдать значительный упадок сервисов и вымирание ссылок. Нормы, направленные на удаление информации или исключение определенных результатов поиска, усиливают это явление. Обычный онлайн-контент не пригоден для долгосрочного архивирования и запоминания.

El internet no olvida.

No, dice Stephan Dreyer: muchos archivos en el internet demuestran tener un periodo medio de vida corto y es posible también observar un deterioro significativo en los servicios y una “descomposición” de los enlaces (URL rot, en inglés). Las regulaciones que apuntan a borrar la información o a suprimir determinados resultados de búsqueda refuerzan estos fenómenos. El contenido online convencional no está diseñado para el archivo a largo plazo y, por tanto, para recordar.

MYTH #47

Maximilian von Grafenstein

Data protection law is about controlling data.

Myth: Data protection law is about controlling personal data. This is already suggested in the notion of "data protection" law and in the famous sentence that individuals shall have "a right to determine the disclosure and usage of 'their' data". A prominent example of this is the view that each kind of personal data may be processed only if individuals (to which the data relate) have given their consent.

Busted: The myth that individuals have a right to control "their" personal data (instead of the risks caused by data processing) sources its power from a very intuitive understanding: If I can control the data that relate to me in one or another way, then I can also control the risk that the data is abused. However, both in daily life and in theoretical reflections, the focus on the data per se often leads to the situation that the actual problem, i.e. the risk of abuse, gets overseen. This leads to a protection that is both excessive and ineffective. A tragic result. Two examples may illustrate this observation:

In data protection law, a person's consent is often seen as the central normative tool for individual self-determination in a digitized world. However, most people will also agree that consent, in its current form applied in practice, does not achieve this aim. Instead of enabling individuals to make a self-determined decision, they are trying to find their daily way through a myriad of consent forms clicking them away (unread). There are many reasons for this so-called consent fatigue. However, one key reason is that individuals consent to everything and nothing: Consents are required everywhere while the consequences of giving the consent (i.e. the actual risks) remain unclear.

Tightly connected to this phenomenon is the overload of information given to individuals on the basis of transparency requirements in data protection frameworks. Often, such information focuses on the data collected from the individuals, while the consequences of its processing remain vague. Further, there is so much collected data that individuals do not see the forest for the trees and ask themselves the question: What kind of information is relevant to me? Thus, focusing on data instead of risks that are caused by data processing to the individual distracts normal users and shifts theoretical concepts of protection away from what is relevant.

In recent discussions, this point of view even runs the risk to be applied to new progressive approaches that aim to solve the problem on a more structural level: Data fiduciaries, for instance, may enforce data protection rights on behalf of individuals; even more far-reaching is the idea that individuals shall have a property right on "their data" so that they can better profit from the data (e.g. by data sale). These new approaches will fail as long as the actual problem is lost out of sight: the risk that data may be misused.

Truth: Data protection law controls the risks to individuals that are caused by the processing of data (not data as such). This difference may seem subtle, but it has far-reaching effects on the reach and limitations of protection. To effectively implement data protection instruments, such as an individual's consent and measures of transparency, one must focus on the consequences of the data processing.

■ ***Source***

Maximilian von Grafenstein, The Principle of Purpose Limitation in Data Protection Laws: The Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation (Baden-Baden: Nomos, 2018).

MYTH #47

Beim Datenschutzrecht geht es um die Kontrolle von Daten.

Nein, sagt Maximilian von Grafenstein: Das Datenschutzrecht regelt die Risiken für Personen, die durch die Verarbeitung von Daten (und nicht durch die Daten als solche) entstehen. Dieser Unterschied mag gering erscheinen, hat jedoch weit reichende Auswirkungen auf die Grenzen des Schutzauftrags. Um datenschutzrechtliche Instrumente wie die Einwilligung einer Person und Maßnahmen zur Transparenz wirksam umzusetzen, muss man sich stets auf die Folgen der Datenverarbeitung konzentrieren.

قانون حماية البيانات يُعنى بالتحكم البيانات.

كلا، هكذا يقول ماكس فون غرافنشتاين: ينظم قانون حماية البيانات المخاطر التي يتعرض لها الأفراد نتيجة معالجة البيانات وليس البيانات في حد ذاتها. وقد يبدو هذا الاختلاف دقيقًا، لكن له آثارًا بعيدة المدى على نطاق الحماية ومحدودياتها. يجب علينا التركيز على آثار معالجة البيانات من أجل تنفيذ فعال لأدوات حماية البيانات، كموافقة الفرد وتدابير الشفافية.

数据保护法是关于控制数据的法律。

不，Maximilian von Grafenstein 写道：数据保护法控制因处理数据（严格来说，并非数据）产生的个人风险。这种差异可能看起来很微妙，但它对保护的范围和局限性具有深远的影响。为了有效地运用数据保护工具，例如个人同意和透明度的测量，必须关注数据处理的结果。

La loi sur la protection des données concerne le contrôle des données.

Non, écrit Maximilian von Grafenstein: la loi sur la protection des données contrôle les risques, pour les personnes, associés au traitement des données (pas les données en tant que telles). Cette différence peut sembler subtile, mais elle a des effets considérables sur la portée et les limites de la protection. Pour mettre en œuvre efficacement des instruments de protection des données, tels que le consentement d‘un individu et des mesures de transparence, il convient de se concentrer sur les conséquences du traitement de ces données.

Закон о защите данных направлен на управление данными.

Это не так, говорит Макс фон Графенштейн: Закон о защите данных контролирует риски для отдельных лиц, вызванные обработкой данных (не данных как таковых). Эта разница может показаться едва уловимой, но она имеет далеко идущие последствия для охвата и ограничений защиты. Чтобы эффективно задействовать инструменты защиты данных, такие как согласие отдельных лиц и меры прозрачности, необходимо сосредоточиться на последствиях обработки данных.

La finalidad de las leyes de protección de datos es controlar los datos.

No, dice Maximilian von Grafenstein: la legislación de protección de datos controla el riesgo para los individuos causado por el procesamiento de datos (no por los datos en sí mismos). La diferencia puede parecer sutil, pero tiene grandes repercusiones en cuanto al alcance y limitaciones de la protección. Para poder implementar instrumentos de protección de datos de forma efectiva, tales como el consentimiento individual y medidas de transparencia, es necesario centrarse en las consecuencias del procesamiento de datos.

MYTH #48

Mark Perry

Information wants to be free.

Myth: The innate nature of information is to self-disseminate. It should be without cost and it should be accessible. Reputable scholars seek open access, and those criticizing intellectual property and supporting free information even take this assumption as excuses for hacking.

Busted: Of course, information itself doesn't want to do anything, it is all driven by the will of people. Since the time individuals have understood that they hold information, they have known of its use and may have given it to others as a valuable asset. (→ #9) Although legal systems have been loath to propertize raw data as this would lead to restraints on normal daily living, the openness provided for information sharing has been eroded over the centuries by concepts of privacy, database protection (Europe), data protection, and various other mechanisms, such as confidential information laws, that restrict sharing. Some data, e.g. that supplied by drug companies for the purposes of regulatory examination of a new product, is also protected. (→ #40) On the other hand, and this perhaps is one of the roots of one form of the "information wants to be free" meme, is the reduction in the cost of sharing information and giving widespread accessibility through the Internet. What would have taken years of work and large sums of money to disseminate can now be made available to half the world at the click of a mouse.

The idea that information could be shared without detriment to the sharer of information has come up in a number of earlier computer law cases, mostly denying the ability of prosecutions to claim "theft" of information (as no deprivation), or the failure of copyright over assemblages of data. These have led to changes in the law ranging from database protection in the European Union to the widespread adoption of anti-hacking laws. The latter have typically criminalized the entry into systems for the purposes of accessing information, changing it or deleting it. The trend has been to allow those with access to data to collect information about everything, and then sell the material to those interested. Often such sales are restricted by contract to prevent the "sharing" of the data, although the data itself may not be protected by any intellectual property laws.

Truth: Useful data is rarely free, neither in the sense of cost nor legal access. Information is being gathered, collated and analyzed at an unprecedented rate. Most of this data diving activity is by governments and corporations who wish to gain advantage or influence over the behaviour of the individuals whose information has been collected. It might rather be the people who want to be free, like Cory Doctorow put it.

Source

Graham Greenleaf, An Endnote on Regulating Cyberspace: Architecture vs Law? 52 (1998) 21 (2) UNSW Law Journal, 593, http://www.austlii.edu.au/cgi-bin/viewdoc/au/journals/UNSWLawJl/1998/52.html?context=1;query=%22information%20wants%20to%20be%20free%22; Steven Levy, "Hackers" and "Information wants to be Free", Medium (2014), https://medium.com/backchannel/the-definitive-story-of-information-wants-to-be-free-a8d95427641c.

MYTH #48

Information will frei sein.

Nein, sagt Mark Perry: Nützliche Daten sind selten kostenlos, und zwar weder im Sinn von finanziellen Kosten noch im Sinn eines einfachen rechtmäßigen Zugangs. Informationen werden in beispiellosen Mengen und mit hoher Geschwindigkeit gesammelt, zusammengestellt und analysiert. Die meisten dieser Datensammelaktivitäten werden von Regierungen und Unternehmen durchgeführt, die sich Vorteile oder Einfluss auf das Verhalten jener Bürger*innen verschaffen wollen, deren Daten gesammelt wurden. Es ist vermutlich also eher der Mensch, der frei sein will, um es mit den Worten von Cory Doctorow zu sagen.

المعلومات يجب أن تكون مجانية/ حرة.

كلا، هكذا يقول مارك بيري: نادرًا ما تكون البيانات المفيدة مجانية سواء من حيث التكلفة أو الولوج القانوني. يتم جمع المعلومات ومقارنتها وتحليلها بمعدل لم يسبق له مثيل. يتم معظم هذا النشاط المتعلق بمعالجة البيانات على أيدي الحكومات والشركات الراغبة في الحصول على أسبقية أو التأثير على سلوك الأفراد الذين جُمعت معلوماتهم. وعلى العكس فقد يكون الأفراد هم الذين يريدون أن يكونوا أحرارًا، كما قال كوري دوكتورو.

以后信息可能会免费。

不，Mark Perry 写道：有用的数据很少是免费的，无论就成本还是合法访问权限来说。信息正在以前所未有的速度得到收集、整理和分析。大部分数据潜水活动是由希望获得优势或希望影响被收集信息个人的行为的政府和公司开展的。这个观点可能是想要让信息免费的人提出的，就像 Cory Doctorow 所说的那样。

L‘information veut être libre.

Non, écrit Mark Perry: les données utiles sont rarement libres, ni en termes de coût, ni en termes d‘accès légal. Les informations sont collectées, rassemblées et analysées à un rythme sans précédent. La plupart de ces activités de collecte de données sont réalisées par des gouvernements et des sociétés souhaitant obtenir un avantage ou acquérir une influence sur le comportement des personnes dont les informations ont été collectées. Comme Cory Doctorow le souligne, il se pourrait que ce soient plutôt les personnes qui veulent être libres.

Информация хочет быть свободной.

Это не так, говорит Марк Пэрри: Ценные данные редко бывают доступными ни в плане стоимости, ни в плане законного доступа. Информация собирается, сравнивается и анализируется с беспрецедентной скоростью. Большая часть деятельности по сбору данных осуществляется правительствами и корпорациями, желающих использовать и влиять на поведение людей, информацию которых они собрали. Скорее, это люди хотят быть свободными, как выразился Кори Доктороу.

La información desea ser libre.

No, dice Mark Perry: la información útil rara vez es gratuita, tanto en términos económicos como de acceso legal. La información está siendo recogida, recopilada y analizada a un ritmo sin precedentes. La mayoría de estas actividades es llevada a cabo por gobiernos y corporaciones que desean obtener ventaja o influencia sobre el comportamiento de los individuos cuya información ha sido recopilada. Es más probable que sean las personas las que desean ser libres, como lo formula Cory Doctorow.

MYTH #49

Francesca Musiani

Peer-to-peer technology is about sharing files illegally.

Myth: Peer-to-peer (P2P) networking technology is an attractive technology that has spread widely with the rise of file sharing applications such as Napster or WinMX. These are mostly used to share copyrighted music or files. P2P technology thus favours digital "pirates" and illicit file-sharing.

Busted: The term "peer-to-peer" refers to a network of equals or peers – individuals, and machines – who, with the help of appropriate communication and exchange systems, are able to collaborate spontaneously, without requiring central coordination. Due to the massive success of P2P file sharing applications in the early-2000s, P2P is widely believed to be a "pirate"-friendly technology used exclusively for sharing copyright-protected files. However, this networking technology is not only used for file sharing: it was certainly, in its first steps, relegated to this one area, which is the easiest technical option and requires a minimum of human and technical resources in order to be implemented.

However, P2P is also leveraged, and increasingly so, for alternative and legal applications, which can serve several needs of the users/consumers/citizens in today's Internet. P2P services suggest themselves as decentralized alternatives to today's fundamental services and instruments of our networked everyday life: search engines, social networks, online file storage services, video streaming, grid computing, instant messaging, group collaboration.

This is not only due to large-scale technological developments (improvement of the quality of users' Internet connections, amount of disk space available on each computer), but also due to the awareness (either by researchers or by the public) that it is necessary to preserve plurality, variety and the possibility of innovation in today's Internet ecosystem. With, for instance, Google, Facebook or Dropbox each time a user performs a search, exchanges a message with someone or stores a photo album, data is sent and saved to a set of servers before it reaches its intended recipient, helping to build a scenario of content "concentration". On the other hand, taking advantage of P2P's decentralizing potential, other applications aim to meet the same requirements from the point of view of the end user (who therefore continues to compose search requests, share messages and store content), but based on different technical architectures by reconfiguring how data is stored and circulated.

Truth: Despite its strong connotations as a "pirate" technology for the sharing of copyright-protected files, P2P is also used for a number of other applications, including attempts to provide decentralized and perfectly legal alternatives to the Googles and Facebooks of today. P2P is also the backbone of blockchain technology.

Source

Malcolm Campbell-Verduyn (Ed.), Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance. Routledge (2017), https://www.taylorfrancis.com/books/e/9781315211909; Francesca Musiani, "Giants, Dwarfs and Decentralized Alternatives to Internet-based Services: An Issue of Internet Governance", Westminster Papers in Communication and Culture, 10(1) (2015), 81–94, http://doi.org/10.16997/wpcc.214.

MYTH #49

Die Peer-to-Peer-Technologie dient der illegalen Weitergabe von Dateien.

Nein, sagt Francesca Musiani: Die Peer-to-Peer-Netzwerktechnologie (P2P) ist eine attraktive Technologie, die mit dem Aufkommen von Filesharing-Anwendungen wie Napster oder WinMX, die in erster Linie zum Teilen urheberrechtlich geschützter Musikstücke oder Daten genutzt wurden, weite Verbreitung erfahren hat. P2P wird daher stark sowohl mit „Pirat*innen“ als auch mit „Filesharing“-Technologie assoziiert. P2P wird jedoch auch für eine Reihe anderer Anwendungen genutzt, darunter den Versuch, dezentrale und vollkommen legale Alternativen zu den Googles und Facebooks unserer Zeit anzubieten und bildet das Rückgrat der Blockchain-Technologie.

تكنولوجيا النظير إلى النظير تُعنى بتشارُك الملفات بالمخالفة للقانون.

كلا، هكذا تقول فرانشيسكا موسياني: أصبحت تكنولوجيا شبكات النظير إلى النظير (P٢P) تكنولوجيا جذابة لعامة الناس مع انتشار تطبيقات تشارك الملفات مثل Napster أو WinMX التي كانت تُستخدم غالبا لتشارُك الموسيقى أو الملفات المحمية بحقوق الطبع والنشر، لذلك قد تحمل فتكنولوجيا النظير إلى النظير دلالات سلبية باعتبارها تكنولوجيا «قرصنة» و«تشارُك ملفات». ومع ذلك تُستخدم تكنولوجيا النظير إلى النظير أيضًا في عدد من التطبيقات الأخرى التي من بينها محاولات توفير بدائل لامركزية وقانونية تمامًا لتطبيقات Google وFacebook اليوم، كما أنها العمود الفقري لتكنولوجيا البلوك تشين.

点对点技术是指非法共享文件。

不，Francesca Musiani 写道：随着主要用于共享受版权保护的音乐或文件的 Napster 或 WinMX 等文件共享应用程序的推广，点对点 (P2P) 联网技术已经成为对普通大众具有吸引力的技术。因此，作为“盗版”和“文件共享”技术，P2P 都具有强大的内涵。但是，P2P 还被用于许多其他应用程序，包括试图为当今的谷歌和 Facebook 提供分散但完全合法的替代方案，此外 P2P 还是区块链技术的支柱。

La technologie peer-to-peer consiste à partager des fichiers illégalement.

Non, écrit Francesca Musiani: la technologie de réseau peer-to-peer (P2P) est devenue attractive pour le grand public grâce à la multiplication d‘applications de partage de fichiers telles que Napster ou WinMX, qui étaient principalement utilisées pour partager de la musique ou des fichiers protégés par le principe des droits d‘auteur. En conséquence, le P2P est considéré à la fois comme une technologie de « piratage » et de « partage de fichiers ». Toutefois, le P2P est également utilisé pour de nombreuses autres applications, notamment pour tenter de fournir des alternatives décentralisées et parfaitement légales aux Google et Facebook d‘aujourd‘hui, et il constitue le pivot de la technologie blockchain.

Технология одноранговой связи – это незаконный обмен файлами.

Это не так, говорит Франческа Мусиани: Сетевая технология одноранговой связи (P2P) стала интересна для широкой общественности с распространением таких приложений для обмена файлами, как Napster или WinMX, которые в основном использовались для обмена защищенными авторским правом файлами и музыкой. Поэтому P2P имеет сильный оттенок как «пиратской», так и «файлообменной» технологии. Однако, P2P также используется для ряда других целей, включая попытки предоставить децентрализованные и совершенно законные альтернативы современным Google и Facebook. P2P также является основой технологии блокчейна.

La función de las tecnologías de comunicación entre pares (peer-to-peer) es compartir archivos de manera ilegal.

No, dice Francesca Musiani: la tecnología de conexión peer-to-peer (P2P) adquirió popularidad entre el público general con la proliferación de aplicaciones de intercambio de archivos o ficheros como Napster o WinMX, las cuales eran utilizadas sobre todo para compartir música o archivos sujetos a derechos de autor. En consecuencia, el P2P tiene fuertes connotaciones tanto como tecnología de “piratería” como de “intercambio de archivos”. Sin embargo, el P2P también se usa para varias otras aplicaciones, incluyendo intentos de proveer alternativas descentralizadas y perfectamente legales a los Googles y Facebooks de hoy en día, y es la columna vertebral de la tecnología de cadena de bloques (blockchain, en inglés).

MYTH #50

Martin Florian

Blockchains will solve all our problems.

Myth: “Blockchain”, the nebulous technology powering Bitcoin and other cryptocurrencies, has wide-ranging applications to all areas of life. Because of its successful application to the realization of digital currencies, it is also perfectly suited for “decentralizing” a wide range of other applications and services, eliminating the need for intermediaries and trust.

Busted: If you are using “Blockchain” as a synonym for “digitization” or “something with computers and cryptography”, then there might be some truth to this myth for you! All caveats about applying technological solutions to complex human problems still apply, of course.

But what does “Blockchain” actually mean? In its narrowest sense, a blockchain is a way of organizing data, a so-called data structure. It’s a list of “things” grouped into “blocks”. Each new block is placed on top of the last one, and you are not allowed to change or remove old entries. The “placing on top” is secured using cryptography. Each block “points” to its predecessor, and by knowing the “correct last block”, we can check whether the data we have of all preceding blocks is in its original form. This is quite useful if you want to ensure that a log of events has not been tampered with. However, someone can easily construct a fake chain of blocks to hide modifications he made. So how do you decide which chain to trust?

Enter Bitcoin. Bitcoin (as well as some of the projects it inspired) attempts to solve a very specific problem: how can a group of anonymous and untrusted peers securely agree on the “correct” chain of blocks? This is very hard. For example, you cannot just vote, because generating fake votes is easy when everyone is anonymous. Roughly, Bitcoin attempts to solve its very hard problem using a “one vote per wasted unit of electrical energy” policy.

Chances are, you are not dealing exclusively with anonymous untrusted peers. So you could explicitly define a group of peers with voting rights, and still use blockchain-the-data-structure. You’ll get a form of distributed database, something that can be made very efficient if your peers can agree on a leader or “being able to call it Blockchain” is not a requirement.

But perhaps “Smart Contracts” will help us to decentralize everything? Unfortunately, they are only helpful for working with data that is already on a blockchain. Ensuring that the data was correct in the first place is still an outstanding and very hard problem. After all, the blockchain is just a chain of blocks—how should it know whether the sun is shining outside or the bananas I’m eating are really fair trade?

Truth: The ideas behind Bitcoin are interesting for groups of peers that want to collaboratively maintain an event log but can’t agree on a single entity to order the log entries. Outside of this narrow scope, blockchain-based systems usually perform worse (in terms of throughput, latency, cost) than existing and simpler approaches. As for trustlessness - a blockchain might help us to ensure that captured data has not been altered, but it cannot tell us whether the data was correct in the first place.

Source

Karl Wüst and Arthur Gervais, Do you need a Blockchain?, 1st Crypto Valley Conference on Blockchain Technology (2018), https://eprint.iacr.org/2017/375.pdf, http://doyouneedablockchain.com; Florian Tschorsch and Björn Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Communications Surveys & Tutorials 18 (2016) 3, https://eprint.iacr.org/2015/464.pdf.

MYTH #50

Blockchains sind die Lösung für all unsere Probleme.

Nein, sagt Martin Florian: Die dem Bitcoin zugrundeliegenden Konzepte sind für Gruppen von Peers interessant, die gemeinsam ein Ereignisprotokoll unterhalten möchten, sich aber nicht auf eine einzige Entität einigen können, um die Logeinträge zu ordnen. Außerhalb dieses engen Rahmens schneiden Blockchain-basierte Systeme in der Regel (in Bezug auf Durchsatz, Latenz und Kosten) schlechter ab als bestehende und einfachere Ansätze. Hinsichtlich des Problems mangelnden Vertrauens könnte die Blockchain helfen sicherzustellen, dass die erfassten Daten nicht verändert wurden, aber sie kann uns nicht sagen, ob die Daten ursprünglich korrekt waren.

البلوك تشين ستحل جميع مشاكلنا.

كلا، هكذا يقول مارتن فلوريان: انبثقت فكرة بيتكوين من مجموعات أقران يريدون الاحتفاظ بسجل أحداث بشكل تعاوني لكنهم لم يتمكنوا من الاتفاق على كيان واحد لترتيب مدخلات هذا السجل. يصبح أداء الأنظمة المستندة إلى تكنولوجيا البلوك تشين خارج هذا النطاق الضيق أداءً أسوأ (من حيث الإنتاجية ومعدل الانتقال والتكلفة) مقارنة بالنُهج الأبسط المتوافرة حالياً. أما فيما يتعلق بالموثوقية فقد تساعدنا تكنولوجيا البلوك تشين على ضمان عدم تعرض البيانات المُسجَّلة للتحريف، لكن لا يمكنها أن تُخبرنا بما إذا كانت هذه البيانات صحيحة أصلاً أم لا.

区块链会解决我们所有的问题。

不，Martin Florian 写道：对于希望协作维护事件日志，但无法就单个实体对日志条目排序达成一致的同行群体而言，比特币背后的构思很有意思。在这个狭窄的范围之外，基于区块链的系统通常比现有和更简单的方法表现得更差（就传送率、等待时间和成本而言）。至于去信任，区块链可以帮助我们确保收集的数据未被改变，但它无法首先告诉我们数据是否正确。

Les blockchains vont résoudre tous nos problèmes.

Non, écrit Martin Florian: les idées à la base du Bitcoin sont intéressantes pour les groupes de pairs souhaitant gérer de manière collaborative un journal d‘événements, mais qui ne peuvent pas se mettre d‘accord sur une seule entité pour mettre en ordre les entrées du journal. En dehors de ce champ restreint, les systèmes basés sur les blockchains fonctionnent généralement moins bien (en termes de débit, de latence, de coût) que les approches déjà existantes et plus simples. Pour ce qui est du problème de fiabilité, les blockchains pourront peut-être nous aider à nous assurer que les données saisies n‘ont pas été altérées, mais ne pourront pas nous dire si ces données étaient exactes au départ.

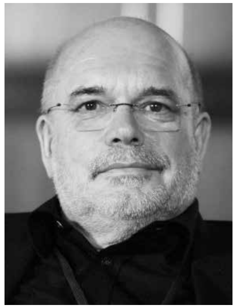
Блокчейн решит все наши проблемы.

Это не так, говорит Мартин Флориан: Идеи, лежащие в основе Биткоина интересны для групп партнеров, которые хотят совместно вести журнал регистрации событий, но не могут ни о чем договориться. За пределами этих тесных границ основанные на блокчейне системы, обычно работают хуже (с точки зрения пропускной способности, времени ожидания, стоимости), чем иные действующие и более простые подходы. Что касается ненадежности – блокчейн может помочь нам гарантировать, что полученные данные не были изменены, но он не может сказать нам, были ли данные верными с самого начала.

Las cadenas de bloques resolverán todos nuestros problemas.

No, dice Martin Florian: las ideas detrás de Bitcoin son interesantes para grupos de pares que desean llevar conjuntamente un registro de eventos, pero no pueden ponerse de acuerdo en una entidad individual para ordenar las entradas de registro. Fuera de este reducido ámbito, los sistemas basados en cadenas de bloques usualmente tienen un desempeño inferior (en términos de rendimiento, latencia y costo) a los enfoques más simples ya existentes. Y en términos de fiabilidad, una cadena de bloque puede ayudarnos a comprobar que los datos recopilados no han sido alterados, pero no puede decirnos si los datos eran correctos en primer lugar.

POSTSCRIPT



Wolfgang Kleinwächter is Professor Emeritus, University of Aarhus, member of the Global Commission on Stability in Cyberspace, former member of the ICANN Board (2013–2015) and former Special Ambassador for the Net Mundial Initiative (2014–2016).

The IGF: the "talking shop" we need for sustainable Internet governance in the age of cyber-interdependence

Wolfgang Kleinwächter

It was the 2005 Tunis Agenda which foresaw a mandate for the Internet Governance Forum (IGF). Governments recognized in the World Summit on the Information Society (WSIS) process that the Internet is a big international issue. But until then they were unable to agree how to "govern" it. China wanted a new intergovernmental body. The US supported private sector leadership. The Working Group on Internet Governance (WGIG), established in 2003 by UN Secretary General Kofi Annan with the mandate to bridge the controversy, proposed a multistakeholder approach. All stakeholders should participate in their respective roles in Internet-related policy development and decision making. But no consensus could be reached.

In Tunis, the risk was high for a failure of the whole summit. Nobody wanted a collapse. Insofar it was not a surprise that governments were looking for a "low-hanging fruit" to make the summit a "success". The establishment of the IGF was this "fruit".

The WGIG's argument for the creation of such a discussion platform was simple: Internet issues are very complex and have technical, political, economic and social dimensions. Before decisions are made, there is a need for a broad discussion to understand this complexity and to recognize the perspectives and arguments of all involved and affected groups: national governments, the private sector (which manages 90 per cent of the Internet applications and services), the technical community (which develops Internet standards and protocols) and the civil society with its billions of Internet users.

Because governments could not agree on giving a new institution Internet-related decision making capacity, they designed the IGF for "discussion only". The fear was that an IGF with a decision-making mandate would turn the platform into a new intergovernmental battlefield. It would block any neutral debates, based on fact and figures. The hope was that a discussion-only platform would open minds and mouths and stimulate a free dialogue among all stakeholders. The knowledge and the wisdom produced in the discussion at the IGF should enable decision-makers to find solutions for Internet-related problems. But decisions should not be made inside the IGF. They should be made by organizations with a mandate to negotiate and decide outside the IGF.

This approach was pragmatic. Indeed, in its 14 years the IGF has evolved into the big annual marketplace for information and ideas around Internet-related technical and political issues. Regardless of the hundreds of Internet conferences which take place every year, there is no other venue where stakeholders on a high level and equal footing from around the globe can have such intense cross-constituency and interdisciplinary conversations. The IGF is a source of inspiration for the way forward into the still unchartered territory of cyberspace.

However, this mechanism also has its weaknesses. There is no procedure in place which channels the messages from the IGF plenaries and workshops into practical processes. There is no landing place for the knowledge and the multistakeholder wisdom, which is collected by the IGF.

20 years ago Internet governance was mainly a technical issue with some political implications. Today, it is a political issue with a technical component. The world has changed. Does it mean that the IGF has to be changed?

The answer is "Yes and No". "No", because there is still the need to understand the complexity of issues before decisions are made. And today´s Internet related issues – from AI to IOT and 5G – are much more complex than the issues discussed in the early 2000s. But "Yes", because there is a need to close the gap between discussion and decision-making.

In 2000, regulating the Internet was not an issue for the majority of intergovernmental organizations. Today it is. The Internet is now on the agenda of more than two dozen global or regional intergovernmental bodies.

Even the WHO and ILO are discussing the consequences of digitalization for the future of work or the improvement of healthcare systems. Cybersecurity is a big issue for negotiations in the 1st and 3rd Committee of the UN General Assembly. Digital trade is on the WTO agenda. The UN Human Rights Council has passed resolutions on privacy and freedom of expression in the digital age.

All those issues are discussed within the IGF. But many of the Internet-related intergovernmental negotiations are not linked to the IGF. Negotiators are sitting in their silos, ignoring what is discussed in the multistakeholder environment of the IGF and reinventing the wheel. This is not only a pity and a waste of resources; it is counterproductive if in a connected world the right hand doesn´t know what the left hand is doing.

As the UN High Level Panel has recently made clear, we live in a world of cyber-interdependence. Interdependence means the need for collaboration among state and non-state actors. And it means that cybersecurity, the digital economy, human rights and technological innovations are interlinked. Only a holistic approach will enable negotiators to find sustainable solutions for a secure, free, open and unfragmented Internet. There is no other place in the world for such a multistakeholder and multidisciplinary dialogue than the IGF.

That is the simple truth: We need a “talking shop“ as a discussion platform, but we need also mechanisms which transfer the IGF wisdom, knowledge and expertise into existing intergovernmental negotiations. The missing link between discussion and decision is a distribution mechanism which sends the messages from the IGF to the OEWG, UNGGE, GGE LAWS, WTO, WIPO, ITU, UNESCO, ILO, WHO, UNCTAD, OECD, G7, G20, BRICS, SCO, NATO, OSCE, ASEAN etc. and invites them to report back to enable and improve enhanced multistakeholder communication, coordination and collaboration on Internet governance.

LIST OF ABBREVIATIONS

G7	Group of Seven
G20	Group of Twenty
AI	artificial intelligence
ASEAN	Association of Southeast Asian Nations
BRICS	Brazil, Russia, India, China and South Africa
CDA	Communications Decency Act
CSNET	Computer Science Network
DNC	Democratic National Committee
DNS	Domain Name System
DoT	DNS over Transport Layer Security
E2EE	end-to-end encryption
GGE LAWS	Group of Governmental Experts on Lethal Autonomous Weapons Systems
HTTPS	Hypertext Transfer Protocol Secure
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	information and communication technologies
IETF	Internet Engineering Task Force
ILO	International Labour Organization
IoT	Internet of Things
IP	intellectual property
ITU	International Telecommunication Union
ML	machine learning
NN	net neutrality
OEWG	Open-ended Working Group
OECD	Organization for Economic Co-operation and Development
OPM	United States Office of Personnel Management
OSCE	Organization for Security and Co-operation in Europe
OSI	Open Systems Interconnection
P2P	peer-to-peer networking technology
SCO	Shanghai Cooperation Organization
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UGC	user-generated content
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNCTAD	United Nations Conference on Trade and Development
UNGGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
USG	United States Government
GDPR	General Data Protection Regulation
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WSIS	World Summit on Information Society
WTO	World Trade Organization

CONTRIBUTORS

Paul Belleflamme
Paul Belleflamme is professor of Economics at Université catholique de Louvain (Belgium). His main research area is theoretical industrial organization, with a special focus on innovation in the digital economy (IPdigIT.eu).

Sebastian Berg
Sebastian Berg is a political theorist and research fellow in the research group “Democracy and Digitization” at the Weizenbaum Institute for the Networked Society in Berlin.

Katharina Bräunlich
Katharina Bräunlich is a post-doctoral researcher at the Department of Computer Science at the University of Koblenz-Landau. Her research focuses on IT security and privacy.

Bernadette Califano
Dr. Bernadette Califano is researcher at the National Scientific and Technical Research Council (CONICET), Science, Technology and Society Center, Maimonides University and National University of Quilmes and Professor of Media Policies at the University of Buenos Aires, Argentina.

Corinne Cath-Speth
Corinne Cath-Speth is a cultural anthropologist and a doctoral student at the Oxford Internet Institute (OII) at the University of Oxford and at the Alan Turing Institute for Data Science and AI.

Michael S. Daubs
Michael S. Daubs is a Senior Lecturer in Media Studies at Victoria University of Wellington in New Zealand.

Tobias Dienlin
Tobias Dienlin is a post-doctoral researcher at the Department of Media Psychology at the University of Hohenheim in Germany. His research is focused on privacy, well-being, and social media.

Martin Dittus
Martin Dittus is a digital geographer at the Oxford Internet Institute with more than a decade of experience in social computing, mass-participation platforms, digital geography, and big data.

Stephan Dreyer
Dr. Stephan Dreyer is Senior Researcher on media law and media governance and head of the research programme “Transformation of Public Communication” at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI), Hamburg.

Johannes Eichenhofer
Dr. Johannes Eichenhofer is a post-doctoral researcher at the University of Bielefeld (Germany), Faculty of Law.

Fabian Ferrari
Fabian Ferrari is a doctoral student at the Oxford Internet Institute, University of Oxford.

Martin Florian
Martin Florian is a senior researcher at the Weizenbaum Institute for the Networked Society in Berlin, where he heads the interdisciplinary research group “Trust in Distributed Environments”.

Bob Frankston
Bob Frankston is a computer engineer and technology pioneer best known for co-creating the first electronic spreadsheet, VisiCalc (rmf.vc/Bio).

Sebastian Gießmann
Sebastian Gießmann is a senior lecturer in Media Studies at the University of Siegen, Germany, and PI of the research project “Digital Network Technologies between Specialization and Generalization” at Siegen’s Collaborative Research Center Media of Cooperation (netzeundnetzwerke.de).

Mark Graham
Mark Graham is a Professor at the Oxford Internet Institute, an Alan Turing Institute Faculty Fellow, a visiting researcher at the WZB Berlin Social Science Centre and the Weizenbaum Institute for the Networked Society, and a Research Associate at the University of Cape Town (markgraham.space).

Nikolas Guggenberger
Nikolas Guggenberger is the Executive Director of the Information Society Project and a Clinical Lecturer in Law at Yale Law School in New Haven, USA.

Amélie P. Heldt
Amélie Heldt is a legal researcher at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI), Hamburg, a doctoral candidate with the University of Hamburg and associated with the Humboldt-Institute for Internet and Society, Berlin.

Paula Helm
Dr. Paula Helm, a postdoctoral fellow in the research project "Structural Transformations of Privacy" at the University of Frankfurt/Main is currently visiting professor at the Surveillance Studies Center, Queens' University, Kingston, Canada.

Sven Herpig
Dr. Sven Herpig is project director for international cyber security policy at the German tech policy think tank Stiftung Neue Verantwortung (SNV) in Berlin.

Sascha Hölig
Sascha Hölig is a Senior Researcher at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI), Hamburg.

Christian Katzenbach
Christian Katzenbach is Senior Researcher at the Alexander von Humboldt Institute for Internet and Society, Berlin, and head of the research programme "The Evolving Digital Society".

Matthias C. Kettemann
PD Dr. Matthias C. Kettemann, LL.M. (Harvard), is head of the research programme "Regulatory Structures and the Emergence of Rules in Online Spaces" at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI), Hamburg, and associate researcher at the Alexander von Humboldt Institute for Internet and Society, Berlin.

Ulrike Klinger
Ulrike Klinger is Professor for Digital Communication at the Institute for Media and Communication Studies at Freie Universität Berlin and head of the research group "News, Campaigns and the Rationality of Public Discourse" at Weizenbaum Institute for the Networked Society in Berlin.

Riikka Kuolu
Riikka Kuolu is an assistant professor of Law and Digitalisation at the University of Helsinki and the director of University of Helsinki Legal Tech Lab.

Emily Laidlaw
Emily Laidlaw is an associate professor in the Faculty of Law at the University of Calgary and is a member of the Institute for Security, Privacy and Information Assurance.

Daniel Lambach
PD Dr. Daniel Lambach is principal investigator of the Heisenberg project "Space, Agency and Practices in the Postnational Constellation" at the Cluster of Excellence "The Formation of Normative Orders", University of Frankfurt/Main.

Claudia Lampert
Dr. Claudia Lampert is a Senior Researcher at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI), Hamburg, with focus on media socialization and health communication.

Suzette Leal
Suzette Leal is a doctoral student at the University of Johannesburg, South Africa. Her research focuses on online engagement in marginalized, impoverished communities.

Philippe Lorenz
Philippe Lorenz is project director for Artificial Intelligence and Foreign Policy at the German tech policy think tank Stiftung Neue Verantwortung (SNV) in Berlin.

Astrid Mager
Astrid Mager is Senior Postdoctoral Researcher at the Institute of Technology Assessment, Austrian Academy of Sciences, and external lecturer at the Department of Science and Technology Studies, University of Vienna.

Jozef Michal Mintal
Jozef is a doctoral candidate at Matej Bel University in Banská Bistrica, Slovakia, a Research Fellow and co-founder of the UMB Data&Society Lab, and a Fellow at the Centre for Media, Data and Society at Central European University.

Katharina Mosene
Katharina Mosene is a political scientist (M.A.) at the Leibniz Institute for Media Research | Hans Bredow Institute (HBI) in Hamburg and a founding member of netzforma* e.V., the association for feminist internet politics and policy.

Francesca Musiani
Francesca Musiani is an associate research professor of the French National Centre for Scientific Research (CNRS) and Deputy Director of its Centre for Internet and Society (cis.cnrs.fr), Paris.

Andrew Odlyzko
Andrew Odlyzko has had a long career in research and research management, including security issues, at Bell Labs and AT&T Labs, and is now a Professor in the School of Mathematics at the University of Minnesota in Minneapolis.

Franziska Oehmer
Dr. Franziska Oehmer is a senior research and teaching associate at the Department of Communication and Media Research DCM, University of Fribourg (CH). She holds a PhD in Communication Science from the University of Zurich and a Bachelor in Law.

Sanna Ojanperä
Sanna Ojanperä is a researcher and doctoral student at the Oxford Internet Institute, University of Oxford and at The Alan Turing Institute and a Future of Work Fellow with the Organization for Economic Co-operation and Development.

Stefano Pedrazzi
Stefano Pedrazzi is a research and teaching assistant and doctoral student at the Department of Communication and Media Research, University of Fribourg (CH). He holds a degree in media and communications science, economics and modern history from the University of Zurich.

Mark Perry
Mark Perry is Professor of Law, and Chair of the Academic Board at the University of New England, Australia, and Emeritus Professor, University of Western Ontario, Canada, where he was Professor of Computer Science.

Ian Peter
Ian Peter is an Internet pioneer and historian. He has been an active civil society representative in Internet Governance developments, including as a Coordinator of the Internet Governance Caucus and the Civil Society Coordination Group.

Amadeus Peters
Amadeus Peters is a criminal law and digitization researcher and a fellow at the Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin.

Roxana Radu
Roxana Radu is a postdoctoral researcher at the Centre for Socio-Legal Studies, University of Oxford, and a Research Associate at the Global Governance Centre, Graduate Institute of International and Development Studies, Geneva.

Sebastian Randerath
Sebastian Randerath studies media and economic studies at the University Siegen, works at the collaborative research center of cooperative media and co-organizes the conference series Pre_Invent on digital cultures, society, technology and art.

Thomas Reinhold
Thomas Reinhold is a computer scientist and fellow at the Institute for Peace Research and Security Policy at the University of Hamburg.

Kate Saslow
Kate Saslow is project manager for Artificial Intelligence and Foreign Policy and International Cybersecurity Policy at the German tech policy think tank Stiftung Neue Verantwortung (SNV) in Berlin.

Kurt M. Saunders
Kurt M. Saunders is a Professor of Business Law at California State University, Northridge.

David Schulze
David Schulze, M.Sc. (Berlin), is a research assistant at the Asia division at Stiftung Wissenschaft und Politik (SWP), the German Institute for International and Security Affairs in Berlin.

Matthias Schulze
Dr. Matthias Schulze is a cyber-security policy researcher at the security division at Stiftung Wissenschaft und Politik (SWP), the German Institute for International and Security Affairs in Berlin.

Ilja Sperling
Ilja Sperling is a technology consultant for the Ranking Digital Rights project (New America), and a freelance information designer and developer for nonprofit organizations (dadascience.design/portfolio).

Matthias Spielkamp
Matthias Spielkamp is co-founder and executive director of AlgorithmWatch (Berlin), an evidence-based advocacy organization with the goal to critically monitor the use of automated decision-making systems. He holds master's degrees in Journalism from the University of Colorado in Boulder and in Philosophy from the Free University of Berlin.

Alek Tarkowski
Alek Tarkowski is co-founder and President of the Centrum Cyfrowe Foundation, a Polish digital think-and-do tank working to ensure that the Internet is for the people. He is also founding member of Communia, the European Association on the digital public domain, and Creative Commons Poland.

Thorsten Thiel
Dr. Thorsten Thiel is a political theorist and leader of the research group "Democracy and Digitalisation" at the Weizenbaum Institute for the Networked Society in Berlin.

Tommaso Venturini
Tommaso Venturini (tommasoventurini.it) is researcher at the CNRS Centre for Internet and Society in Paris. He is also associate researcher of INRIA and of the médialab of Sciences Po Paris and founding member of the Public Data Lab (publicdatalab.org).

Daniel Voelsen
Dr. Daniel Voelsen is researcher in the global issues division at Stiftung Wissenschaft und Politik (SWP), the German Institute for International and Security Affairs in Berlin.

Maximilian von Grafenstein
Prof. Dr. Maximilian von Grafenstein, LL.M., is Professor for Digital Self-Determination at the Einstein Center Digital Future, University of the Arts in Berlin, and co-head of the research programme "Data, Actors, Infrastructures: Governance of Data-Driven Innovation and Cyber-Security" at the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin.

Robin Tim Weis
Robin Tim Weis, M.A. (Heidelberg), is a Senior Project Manager at the Office of Science and Technology Austria - OSTA, situated within the Embassy of Austria in Washington DC.

Alina Wernick
Alina Wernick is a researcher at the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin and a doctoral candidate at the Ludwig Maximilian University of Munich.

Laeed Zaghlami
Prof. Laeed Zaghlami, M.Phil, PhD, is a lecturer at the Faculty of Information and Communication, Algiers University 3 and external examiner at Mauritius University.

Mariano Zukerfeld
Dr. Mariano Zukerfeld is researcher at National Scientific and Technical Research Council (CONICET), Science Technology and Society Center, Maimonides University, and Professor of Sociology of Informatics, University of Buenos Aires.

EDITORS

Matthias C. Kettemann

PD Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard), is senior researcher at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI), head of its research programme on rule-making in online spaces and associated researcher at the Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin. His research focuses on the normative interaction of different stakeholders and various normative orders. He studied international law in Graz, Geneva and Harvard Law School and completed his postdoctoral work at the Cluster of Excellence “The Emergence of Normative Orders” at Goethe University Frankfurt am Main. Matthias has provided expertise for the German Bundestag, several DAX companies, foundations and international organizations on Internet regulation, cybersecurity and human rights.

Stephan Dreyer

Dr. Stephan Dreyer is senior researcher in media law and media governance at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI) and head of a research program on the transformation of public communication. His research focuses on regulatory issues of mediated communication in a datafied society. After studies of law at the University of Hamburg he has become a legal expert in regulatory questions at the intersection of protection of minors, privacy and data protection, he is spokesperson for the Complaint Committee as well as the Expert Committee of the Association of Voluntary Self-Regulation of Digital Media Service Providers (FSM) and child protection expert at the Entertainment Software Self-Regulation Body (USK online) .

IMPRINT

ISBN 978-3-87296-150-1 (print)
ISBN 978-3-87296-154-9 (E-Book)
Kettemann, Matthias C.; Dreyer, Stephan (2019):
Busted! The Truth about the 50 Most Common Internet Myths.
Hamburg: Verlag Hans-Bredow-Institut

Editors
Matthias C. Kettemann
Stephan Dreyer

Design and Layout
Vagedes & Schmid GmbH

Translation
TypeTime Translations GmbH, Hamburg

Printing
Druckerei Gläser · Blücherstraße 22 · 10961 Berlin

Verlag Hans-Bredow-Institut
Rothenbaumchaussee 36
20148 Hamburg
verlag@leibniz-hbi.de
https://leibniz-hbi.de

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

LEIBNIZ-INSTITUT
FÜR MEDIENFORSCHUNG
HANS-BREDOW-INSTITUT