2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

Net Neutrality in the Context of Cyber Warfare

Kim Hartmann
Conflict Studies Research Centre
Oxford, United Kingdom
kim.hartmann@conflictstudies.org.uk

Keir Giles
Conflict Studies Research Centre
Oxford, United Kingdom
keir.giles@conflictstudies.org.uk

Abstract: Real or potential connections between infrastructure of different security levels, from relatively unprotected individual users up to interfaces with critical national infrastructure, have made cyberspace a highly contested and congested domain. But operating conditions within this domain strongly favour malicious actors over legitimate operators seeking to provide security and protect systems and information. Technical capabilities to establish dominance and cause damage in this domain are widely distributed, but legal and ethical constraints prevent legitimate actors from using them to their full potential.

Within this context, net neutrality presents a limiting factor on the capability of legitimate actors to respond to harmful activity in cyberspace whose common aim is to install and uphold a technical imbalance. Under the principle of net neutrality, each data packet must be transmitted with equal priority, irrespective of its source, destination, content or purpose. This is disadvantageous to cyber defence. Comparisons to jungle or arctic warfare, where operating conditions are neutral and degrade the performance of each combatant side equally, are invalid, as malicious operators are capable of technically manipulating data traffic to their favour. While both malicious and legitimate actors may have comparable capabilities, legitimate actors are bound to legal and political restrictions, making them immobile in several cyber warfare scenarios. Transferring the principles of net neutrality to real life scenarios corresponds to depriving military, police and emergency operators from any privilege that allows them to respond to an incident – in effect, depriving them of their blue lights and emergency powers even in severe incidents targeting critical infrastructure that may threaten civilian lives.

This paper investigates the potential opportunities and challenges of an adjustment to the principle of net neutrality to facilitate defensive action by legitimate actors; how this adjustment could contribute to regaining control in congested cyber domains

in the case of national or international cyber incidents; and the risks associated. The different ways of dealing with net neutrality in cyber defence situations in the EU, UK and Russia are compared. Particular focus is put on the organisations and capabilities needed to establish technical sovereignty in multi-domain networks, including consideration of the acceptability of outsourcing the task of upholding cyber sovereignty to external institutions.

Keywords: *net neutrality, cyber defence, cyber security, net regulation*

1. INTRODUCTION

The long-running debate over net neutrality gained unprecedented prominence in public attention during the autumn of 2017 as United States Communications Commission (FCC) chairman Ajit Pai proposed the repeal of policies dating from 2015 that safeguarded net neutrality in the US. The public discussion on net neutrality was primarily concerned with potential abuse and the prospect of forming and protecting positions within specific markets such as the telecommunications sector; a situation exacerbated in the United States in particular by limited consumer choice resulting from a small number of major telecommunications companies already enjoying near-monopoly status.[1] This threat would not only affect the telecommunications market and its service providers, but also any other market or services depending on communication through Internet Service Providers (ISPs) – in effect, any area of modern business. The most prominent and intensively discussed examples of services which faced severe disruption were social media and streaming platforms, both of which derive clear benefits from neutral treatment of Internet traffic because of their data-heavy nature and vulnerability to any increase in the cost of data transfer.

It is likely that the involvement of these platforms in the debate, augmented by their substantial presence in everyday civil life, ignited the mainly emotion-driven debate on the 'freedom of the Internet'. This topic rapidly eclipsed the technical aspects of net neutrality overhaul. Comparisons were often made to regulations on water and electricity prices. The suggestion that Internet access is an essential service, and therefore should be protected from open market forces, illustrated how net neutrality discussions focus on matters of principle while neglecting technical aspects that challenge a universally connected, digital society.

The concept of net neutrality has predominantly been associated with constraining ISPs from throttling transmission rates and limiting Internet access for end-users. However,

1 Brian Fung, 'FCC plan would give Internet providers power to choose the sites customers see and use', *Washington Post*, November 21, 2017.

this article will consider how net neutrality influences the way data is transferred in cyberspace in a number of other ways. The abolition of net neutrality principles in one country or more provides both opportunities and challenges, affecting the nature of both offensive and defensive computer network operations (CNO) during peacetime as well as overt hostilities.

Real or potential connections between infrastructures of different security levels are established through networking devices and the individuals or organisations that own them. Security levels ranging from relatively unprotected Internet of Things (IoT) appliances, through individual user devices and interfaces up to critical national infrastructure may easily and unnoticeably become interconnected, rendering cyberspace a highly contested and congested domain. But operating conditions within this domain strongly favour malicious actors over legitimate operators, especially as security standards may be legally binding but not technically enforced. This is also observable for net neutrality principles: it is common practice to provide an equal level of Internet service availability to end-users by ISPs and legislation may require compliance with according policies, but there is no technical enforcement. Consequently, malicious actors can abuse net neutrality principles through different attack vectors and use it to hide their actions. While the technical capabilities to establish dominance in the cyber domain are widely distributed, legal and ethical constraints prevent legitimate actors from utilising them to their full potential.

A key common aspect to many CNO attacks is establishing, maintaining and protecting privileged access to systems or processes. Cyber attacks can seek to establish an imbalance between the attacker and the defenders in terms of prioritised access to data, components or networks. As such, net neutrality presents a limiting factor on the capability of legitimate actors to respond to harmful activity in cyberspace. Under the principle of net neutrality, each data packet should be transmitted with equal priority, irrespective of its source, destination, content or purpose. This means that cyber defence, or responses to critical incidents, will not receive any prioritisation over 'normal' traffic, and consequently present an advantage to an attacker seeking to isolate the target of the attack. However, the ability to respond to cyber attacks from any location is crucial to efforts by NATO member states to set up cyber defence units capable of cooperating in live cyber operations.[2] Officials must be aware that net neutrality principles may compromise this effort unless other methods are established to uphold cyber dominance among allies. Examples of such alternative methods may range from dedicated private networks, through hidden network entry points, to organisational and administrative measures.

In effect, interdiction of remote cyber defence efforts by an attacker poses an analogous problem in cyberspace to hostile actors seeking to isolate areas of planned operations

2 NATO, 'Cyber Defence', December 14, 2017, https://www.nato.int/cps/en/natohq/topics_78170.htm.

by means of advanced anti-access and area denial (A2AD) systems, preventing access by NATO reinforcements seeking to defend them. But while in air, sea or land operations, friendly forces can take advance steps to ensure privileged access in time of crisis,[3] in cyberspace the principles of net neutrality prevent any such pre-emption.

While communications transferred through separate networks independent of civilian ISPs are unlikely to be affected (such as would be expected in military operations), CNO against critical infrastructure and cyber espionage have already been conducted through the public Internet, open for access to all.[4] With critical infrastructure a likely target in cyber warfare, legitimate cyber actors must be capable of effectively and remotely counteracting sophisticated cyber attacks.[5] This remote access to attacked network components could be enabled by physically separate communication lines as physical backdoors to the network (economically unfeasible in almost all cases) or allowing data traffic to be tunnelled. However, the latter does not guarantee that communication is possible in a congested domain as components and routes may be inoperative or compromised. Prioritising traffic through ISPs, by contrast, could allow network administrators to identify the tunnelled communication and install in advance packet-based rules that enable critical communication even during attacks.

Comparisons to jungle or arctic warfare, where operating conditions are neutral and degrade the performance of each combatant side equally, are invalid since the operating conditions in cyberspace can be adapted by one side or the other. Skilled cyber actors are capable of ensuring that their data traffic is prioritised or that the opponent's traffic is downgraded or blocked. Additionally, the opponent in a cyber warfare scenario may not only target military components but also potentially attack civilian critical infrastructures, forcing governments to respond immediately to ensure the safety of their citizens and prevention of crippling or catastrophic damage. Therefore, transferring the principles of net neutrality to real life scenarios would rather correspond to depriving military, police and emergency operators of any privilege that allows them to respond promptly to an incident – in effect, taking away their blue lights and emergency powers even in military operations or severe incidents targeting critical infrastructure that may threaten civilian lives. A more appropriate analogy would be a car chase where criminals can run red lights and set up roadblocks, but the police must still observe traffic rules and speed limits.

Net neutrality is currently not technically enforced, nor has it ever been. There are no central authorities capable of monitoring and enforcing net neutrality on global networks. Additionally, even when legislation demands the enforcement of net neutrality policies, no guarantees can be given once traffic is routed outside national

3 Daniel Fiott, 'Towards a "military Schengen"?', EU Institute for Security Studies, November 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2031%20Military%20Schengen.pdf.

4 National Cyber Security Centre (NCSC), last access: January 7, 2018, https://www.ncsc.gov.uk/index/alerts-and-advisories.

5 Thomas A. Johnsson (Ed), *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, 1st Edition, CRC Press, April 16, 2015, ISBN: 978-1482239225.

borders. The management of data traffic has always been the responsibility of telecommunication organisations and network administrators. Routing rules based on packet origins, content, frequency and general network load are common practice in most networks. This has not been a problem as long as fast communication appeared cheap and unlimited, and large-scale cyber attacks remained the preserve of science-fiction novels or far-fetched 'cyber Pearl Harbor' predictions. While some corporate entities may very plausibly have the intention of abusing the new regulatory situation in the United States for financial benefit, there is also a need for a rational and problem-oriented discussion on how to handle network traffic management in the future with the rising challenges of cyber warfare in mind.

Hence the remainder of this paper investigates the potential opportunities and challenges of an adjustment to the principle of net neutrality to facilitate defensive action by legitimate actors; how adjustments may allow actors to gain control in congested cyber domains in the case of national or international cyber incidents; and risks associated with weakening of net neutrality principles. The different ways of dealing with net neutrality in the EU, UK and Russia are considered. Particular focus is put on the organisations and capabilities needed to establish technical sovereignty in multi-domain networks, including consideration of the acceptability of outsourcing the task of upholding cyber sovereignty to external institutions.

2. NET NEUTRALITY IN THE EU, UK AND RUSSIA

This section explores principles under which ISPs may legitimately interfere with network traffic by technical means in order to illustrate the opportunities and challenges of weakening net neutrality overall. Three different regulatory environments (the EU, UK and Russia) are compared to illustrate the wide variations in philosophy and enforcement between different jurisdictions.

A. Net Neutrality

In simplistic terms, net neutrality means that network providers must treat all network traffic equally and may not interfere with data traffic in a way that affects the traffic of selected parties only. Net neutrality is a set of principles, not a technical implementation. In fact, due to the need of modern networks to be able to cope with data transmission errors and delays, most communication protocols are designed to deal with limitations without end-users noticing. In other words, their design renders them capable of hiding net neutrality violations. This is part of what opens network communications to abuse in hidden cyber operations and creates the huge imbalance between legitimate actors bound to net neutrality on the one hand, and malicious actors with no effective constraint by the rule of law on the other.

Computer networks consist of components, which in turn have physical and logical entities, all of which can communicate between themselves. In order to be able to connect components of completely different architectures, purposes, languages and communication types, the ISO OSI standard was developed.[6] This is a conceptual model that defines how 'data' is organised and communicated on different abstraction layers, moving from physical representations to logical units. An ISP provides the core physical components within a network[7] and as a result has access to the complete OSI stack. ISPs are capable of interfering with traffic on any layer: cutting the physical connection, dropping packets, filtering for services and (unencrypted) content in data, and more.

Net neutrality advocates have been concerned with ISPs throttling down transmission rates, while their opponents put forward counter-arguments of innovation of better bandwidth distribution techniques and networking technologies that are incompatible with net neutrality principles. It is currently impossible to predict how ISPs will handle traffic in the future if net neutrality principles are weakened, but the status quo leads to educated guesses on future network management techniques, such as:

- The pure 'throttling' of data traffic based on origin or destination is commonly associated with dropping packets. By dropping packets, the quality of the single connection may go down, while the overall bandwidth is improved: the ISP regains some of its bandwidth by not servicing one of its customers.
- Another way of gaining bandwidth is by queuing packets. Packets are not 'lost' but take longer to be delivered as they are not forwarded immediately. Again, the ISP gains bandwidth by reducing processing time.

Selection of which traffic to interfere with may be based on packet, service or content information. Depending on the type of information chosen, the interference is performed on different layers of the network stack and may require additional methods such as deep packet inspection (DPI). DPI has been associated particularly with Internet censorship,[8] but is also a common tool for cyber forensics and network administration.

However, methods that alter bandwidth distribution merely by dropping or queuing are not suitable to guarantee privileged data transmissions for selected customers or services, as solutions exist to avoid dropping, queuing and DPI. The most prominent example known to be adopted to avoid censorship (which is usually also based on these methods) is the use of virtual private networks in combination with so-called

6 Andrew S. Tanenbaum, David J. Wetherall, *Computer Networks*, 5th Edition, Pearson, January 9, 2010, ISBN: 978-9332518742.

7 Barry Raveendran Greene, Philip Smith, *Cisco ISP Essentials*, Cisco Press – Networking Technology Series, April 16, 2002, ISBN: 978-1587050411.

8 Ralf Bendrath. 'Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection.' International Studies Association Annual Convention. Vol. 15. No. 18. 2009.

'onion routing' networks such as the Tor network.[9] It is therefore more than likely that alternative methods will be used.

The relevance to cyber warfare lies in the fact that, in addition to simple destructive potential, cyber attacks commonly serve the purpose either of gathering information or of exerting power through the medium of the Internet. This can be through achieving and demonstrating interdiction or malfunctioning of networks and their associated services. While current attacks tend to aim at specific network components, it is likely that future attacks will be directed against bandwidth distribution technologies.

Several already-common attack types include methods that abuse net neutrality principles to ensure a larger portion of bandwidth is available to the attacker. This provides a number of secondary effects for any botnet or distributed attack. It allows an attacker to undertake further activities in parallel, unaffected by the ongoing attack itself; it demonstrates power in the domain; it creates an impression of omnipresence of the attacker; it hijacks the bandwidth of legitimate actors; it disables the attacked components; and finally, and most significantly for the current discussion, it hampers external interference by legitimate cyber defence actors as the attacked components may become inaccessible.

B. EU

In September 2013, the European Commission published a draft set of regulations for the telecommunications single market. This draft was heavily criticised for not sufficiently addressing net neutrality regulations and for introducing differentiation between 'communications access' and 'specialised services access' without specifying these services adequately. The draft was adjusted and approved by the EU parliament in April 2014.[10]

The adjusted draft specifically declares that Internet service access:

> 'means a publicly available electronic communications service that provides connectivity to the Internet in accordance with the principle of net neutrality, and thereby connectivity between virtually all end points of the Internet, irrespective of the network technology or terminal equipment used'.[11]

9 The Tor project, https://www.torproject.org/, last access: January 8, 2018. See also McCoy, D., Bauer, K., Grunwald, D., Kohno, T. & Sicker, D. 'Shining light in dark places: Understanding the Tor network'. In *Proceedings of the 8th International Symposium on Privacy Enhancing Technologies* (pp. 63-76). Springer, Berlin, Heidelberg, July 2008.

10 EU Parliament, 'Draft on the proposal for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/22/EC, and Regulations (EC) No 1211/2009 and (EU) No 531/2012', March 20, 2014.

11 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0281+0+DOC+XML+V0//EN.

Net neutrality is defined as the:

> 'principle according to which all Internet traffic is treated equally, without discrimination, restriction or interference, independently of its sender, recipient, type, content, device, service or application'.[12]

Specialised services are allowed for that are:

> 'provided over logically distinct capacity, relying on strict admission control, offering functionality requiring enhanced quality from end to end, and that is not marketed or usable as a substitute for Internet access service'.[13]

In other words, specialised services are considered as supplementary offers to Internet access services. Examples of such services could be real time applications, sensory data aggregations or distributed computing services.

Following heated discussion, the 2014 draft was further adjusted and approved in November 2015 as EU Regulation 2015/2120.[14] The guidelines for implementation of the April 2014 draft no longer included the term 'net neutrality'. ISPs are still required to follow the 'best effort' principle, requiring all packets to be treated equally (in other words, a core aspect of net neutrality). However, permission for 'zero rating' and a specification of 'sufficient data traffic management' methods have both been criticised. Although violations of net neutrality principles through the use of DPI is possible, several ISPs in EU states are known to use DPI in varying contexts. DPI is known to be carried out by governments and their legitimate actors. The inspection results are used for further processing, prosecution and surveillance.

Zero rating refers to the practice of not imposing additional costs for access to selected online services, while all others incur such charges. The application of this approach varies widely across Europe. The Netherlands enforced a strict net neutrality policy, but at the other extreme, in Portugal ISPs offer a strictly limited connection service with additional charges for access to a wide range of common applications.[15] These charges are usually in the form of purchasing specific packages, named for example 'social' or 'music', which include services selected by the ISP; the criteria

12 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BAMD%2BA8-2015-0300%2B014-024%2BDOC%2BPDF%2BV0%2F%2FEN.

13 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0281+0+DOC+XML+V0//EN Chapter 1, Article 2 (15) in reference 10.

14 Official Journal of the European Union, Regulation 2015/2120 of The European Parliament and Council, November 25, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&rid=2, last access: January 8, 2018.

15 *The Guardian*, 'Net neutrality enshrined in Dutch law', June 23, 2011, https://www.theguardian.com/technology/2011/jun/23/netherlands-enshrines-net-neutrality-law, last access: January 7, 2018; Alex Hern, 'Net neutrality: why are Americans so worried about it being scrapped?', *The Guardian*, 22 November 22, 2017, https://www.theguardian.com/technology/2017/nov/22/net-neutrality-internet-why-americans-so-worried-about-it-being-scrapped, last access: January 7, 2018.

for selection include the profitability of each service, since the service providers pay a sum to the ISP for inclusion. The 'social' package can, therefore, include Facebook and WhatsApp, while all other social media platforms are not available. The less profitable services cannot be blocked by the ISP, since this would clearly violate net neutrality principles, but they can be de facto excluded by pricing policies. This could, for example, take the form of imposing an indirect cost penalty on users of Telegram by ensuring that data transferred via that app counts against the user's strictly limited 'free' quota, while WhatsApp data has a much higher limit as part of a package.

The 'traffic management' stipulation means that ISPs may adjust data flow rates, for instance to avoid service disruption due to traffic overload. ISPs are reported to have throttled throughput during evening hours (when most customers use their streaming services) to 'encourage' users to stagger demand. Consequently, instead of all customers starting to stream video at, for example, 8 p.m. they do so earlier or later. This allows the ISP to avoid specific traffic peaks, and therefore economise on investment in new hardware that would otherwise be necessary only during a once-a-day data throughput peak. However, this form of management has been criticised as potentially offering a back door to abandoning net neutrality by preferring specific services or traffic.

C. UK

In direct contrast to current developments in the US, the UK government has taken a regulatory approach to ensuring that all UK homes and businesses should have a minimum standard of access to high-speed Internet by 2020.[16] This in itself, however, does not currently prevent the UK's leading ISPs from filtering and blocking Internet content.

In 2014, the *Enemies of the Internet* annual report published by Reporters Without Borders (RSF) listed the UK among the top 14 states where data traffic is monitored, blocked or manipulated.[17] Yet in its 2017 report to the European Commission on compliance with net neutrality regulations, the UK communications regulator Ofcom claimed that 'there are no major concerns regarding the openness of the Internet in the UK.'[18] Those areas identified were minor concerns related primarily to choice of end-users' terminal equipment and zero rating. This apparent contradiction derives from limitations in the EU regulations. In addition to introducing 'sufficient data traffic

16 Paul Sandle, 'Britons will have legal right to high-speed broadband by 2020', Reuters, December 20, 2017, https://uk.reuters.com/article/uk-britain-broadband/britons-will-have-legal-right-to-high-speed-broadband-by-2020-idUKKBN1EE0RS.

17 Reporters Without Borders, annual Report 'Enemies of the Internet 2014', 12 March 12, 2014. See also James Vincent, *The Independent*, 'UK Branded an "Enemy of the Internet" for the first time by Reporters Without Borders', March 17, 2014, https://www.independent.co.uk/life-style/gadgets-and-tech/uk-branded-an-enemy-of-the-internet-for-the-first-time-by-reporters-without-borders-9196571.html, last access: January 7, 2018.

18 'Monitoring compliance with the EU Net Neutrality regulation: A report to the European Commission', Ofcom, June 23, 2017, p. 2, https://www.ofcom.org.uk/__data/assets/pdf_file/0018/103257/net-neutrality.pdf.

management' and 'specialised services', the EU also leaves decisions on whether actions are compliant with the regulations with national courts. As a result, while the Commission may have drafted a regulation on the telecommunications single market that seems to prohibit general filtering, blocking and monitoring of data packets due to net neutrality considerations, in practice implementation of these regulations depends on national jurisdiction. In other words, varying standards of net neutrality can be applied that are still compliant with the EU Regulation and with national law. While Ofcom followed the Commission's regulatory guidelines, RSF applied an ideal image of net neutrality not defined by the EU.

The fact that the landing points of several of the submarine cables that form the backbone of the Internet, especially between Europe and the US, are in the UK is particularly noteworthy. If European net neutrality standards are not carried across into UK law on the withdrawal of the UK from the EU, this will mean that the UK is free to apply its own standards to a substantial proportion of the data that passes between the United States and the EU. Unlike internal developments in the US, this could have a direct effect on the uninterrupted throughput of packets intended for delivery to Europe.

D. Russia

Russia has taken a significantly different approach to net neutrality and to privileging defensive measures compared to the UK, Europe or the US.[19] Most Russian ISPs provide clients with cost-free access to certain websites and services, such as Facebook, Vkontakte, Odnoklassniki, LiveJournal and Yandex Maps.[20] But in addition, governmental privilege is a significant factor in determining access. Many government websites are free to access by law,[21] and by contrast the government has the legal and technical power to disrupt or entirely block access to other Internet resources. According to Russian prosecutor-general Yuriy Chaika, by 2017 around 1,200 websites had been officially blocked under this legislation.[22]

In March 2017 legislation was reported to be under preparation under which Russian courts would be able to punish both domestic and foreign corporations for failing to comply with Russian law by ordering that access to their websites be slowed down.[23] The storage of Russian users' data on Russian servers by foreign Internet companies has been required by law since September 2015, when Law No. 242-FZ,

19 Roman Mirov, 'Конец нейтралитета: как США проиграли битву за интернет,' *Lenta.ru*, January 3, 2018, https://www.gazeta.ru/tech/2018/01/03/11551418/no_net_neutrality.shtml.

20 Sergey Vorniches, 'Всё, что нужно знать о сетевом нейтралитете,' *Apparat.cc*, February 27, 2015, https://apparat.cc/world/about-net-neutrality/.

21 'Доступ к 122 сайтам Рунета сделают бесплатным,' *Известия*, February 24, 2015, https://iz.ru/news/583390.

22 'Russian Police Have Blocked 1,200 Websites Since 2014,' *The Moscow Times*, January 12, 2017, https://themoscowtimes.com/news/1200-russian-websites-blocked-since-2014-56794.

23 Anastasia Golitsyna, 'Для интернет-компаний придумали наказание—замедлять доступ к их сайтам,' Ведомости, March 13, 2017, https://www.vedomosti.ru/technology/articles/2017/03/13/680827-zamedlit-skorost-dostupa.

adopted in 2014, came into force. Compliance with this localisation requirement by Twitter[24] and Snapchat[25] has been claimed by the Russian communications regulator Roskomnadzor but denied by the companies themselves, while Facebook is not yet compliant and consequently is regularly threatened with a nationwide ban.[26] According to a November 2017 survey, Google, Apple, Alibaba, Viber, Gett, Uber and Microsoft all rent Russian data centre space for the purpose of compliance.[27]

All of these measures are in accordance with a predominant view among Russian government agencies, especially those concerned with national security, that the Internet presents more of a threat than an opportunity. In April 2014, President Vladimir Putin remarked that the Internet 'came about as a special project of the CIA' and implied that it continued to be a tool of the US government, and consequently dangerous for Russia.[28] In contrast with Western assumptions, Russian information security preoccupations focus on the role not only of hostile code such as cyber attacks, but also hostile content such as opinions or information which are detrimental to the Russian state.[29] President Putin has personally praised Chinese-style censorship and defended it against criticism from digital rights advocates.[30]

But Russia's plans to protect itself from the Internet go even further, and extend to consideration of operating without access to global Internet services at all.[31] This scenario is variously presented by Russian government officials as either a voluntary withdrawal by Russia – 'pulling the plug' – or being disconnected by the hostile West, which according to one persistent Russian view, controls the Internet.[32] President Putin's adviser on Internet affairs, German Klimenko, is a particular advocate of Chinese-style Internet restrictions and preparing for possible total net withdrawal.[33]

24 Alec Luhn, 'Moscow Says Twitter Ready to Store Data of Users on Russian Servers Despite Concerns Over Surveillance,' *The Telegraph*, November 8, 2017, http://www.telegraph.co.uk/news/2017/11/08/moscow-says-twitter-ready-store-data-users-russian-servers-despite/.

25 Marina Galperina, 'Oops, Snapchat Accidentally Ended Up on a Russian Government Snitch Registry,' *Gizmodo*, August 10, 2017, https://gizmodo.com/oops-snapchat-accidentally-ended-up-on-a-russian-gover-1797721574.

26 'Роскомнадзор пригрозил Facebook блокировкой,' *РБК*, September 26, 2017, https://www.rbc.ru/own_business/26/09/2017/59ca1e899a7947351acdf385.

27 Galina Boyarkova, 'Все терабайты в гости к нам,' *Фонтанка*, November 12, 2017, https://www.fontanka.ru/2017/11/10/144/.

28 'Путин заявил, что интернет - это проект ЦРУ,' *BBC Russian Service*, April 24, 2014, http://www.bbc.com/russian/rolling_news/2014/04/140424_rn_putin_csi_Internet.

29 This contrast is examined in detail in Keir Giles, 'Russia's Public Stance on Cyberspace Issues', in *C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012 4th International Conference on Cyber Conflict.*

30 'Не стоит критиковать китайский вариант ограничений в Интернете – Путин,' *Звезда*, April 3, 2017, https://tvzvezda.ru/news/vstrane_i_mire/content/201704031346-9yin.htm.

31 Grigory Naberezhnov and Darya Luganskaya, 'Кремль прокомментировал сообщения об отключении России от интернета,' *РБК*, September 19, 2014, https://www.rbc.ru/politics/19/09/2014/5704225a9a794760d3d419b6.

32 'Клименко: Россия должна быть готова к отключению от мирового интернета,' *ТАСС*, December 29, 2016, http://tass.ru/obschestvo/3914882.

33 'Советник президента предложил ограничить интернет в России,' *Дождь*, January 26, 2017, https://tvrain.ru/news/Internet-426274/.

In March 2018, Klimenko announced that, after lengthy preparations, Russia was now technically capable of removing itself from the global Internet.[34]

Russia's security-driven approach to managing the Internet stands in stark contrast to the Euro-Atlantic community, and the difference is instructive. We argue in this paper that net neutrality as currently understood by the West is a potential handicap for ensuring security and responding to cyber warfare actions. In Russia, this challenge is well recognised and bound up with the perceived threat of free flow of information across national borders, which for the West is an inalienable element of how the Internet works. The result is that Russia has circumvented the net neutrality challenge by changing the entire basis for Internet access, and making it conditional on state interest. Any solution this extreme would be unpalatable and unworkable in Western liberal democracies, being incompatible both with principles of freedom of expression and with the greater independence of commercial entities including ISPs outside Russia.

3. NET NEUTRALITY AND CYBER WARFARE

Recent net neutrality discussions have centred on censorship, Internet access and traffic limitations. However, these discussions are too narrow and must be expanded to more general considerations on data traffic management, which should be perceived as a core element in future cyber warfare.

A. Net Neutrality in Attack Vectors

Malicious actors can abuse net neutrality to establish dominance through different attack vectors, including DDoS, DrDoS and SYN-flood attacks.

DDoS-attacks use the fact that all incoming traffic is treated equally to create an advantage for the attacker. All IT components have a limit to their processing capabilities, and when legitimate requests to a component compete on an equal basis with a flood of malicious traffic from bots, the component is overloaded and becomes unable to reply. While this principle is a standard tactic, there are many different ways of carrying out a DDoS-attack. In a distributed reflected DoS-attack (DrDoS), the attacker hijacks (spoofs) the IP-address of its target and sends service requests to servers (such as the DNS), asking them to reply to the spoofed IP. What follows is a DDoS-attack with no attribution being possible and, depending on the servers involved, that is impossible to block without self-inflicted damage. One of the largest DDoS-attacks recorded to date was observed during March 2018 against Github, causing a record-breaking data transfer rate of 1.35 Terabits per second using

34 'Советник Путина: Россия готова к отключению от мирового интернета', *RFE/RL*, March 5, 2018, https://www.svoboda.org/a/29079358.html.

a modified DrDoS.[35] In this scenario the attacker also relies on the fact that the target will treat all data packets equally, even when not useful, not requested or identified as potentially harmful.

One of the most basic, yet highly imbalanced methods to attack a network component is a SYN flood attack. SYN flood attacks belong to the group of DoS-attacks that abuse both the equal treatment of packets at the target's side and the TCP handshake protocol. To establish a TCP connection to the target (server-side) from the attacker (client-side), a three-way handshake is initiated. The client sends a SYN-request (synchronise) to the server, the server replies with a SYN-ACK (SYN-acknowledge) and allocates resources for the awaited TCP connection. Usually, the client replies with another ACK, which establishes the TCP connection, however, a malicious client can withhold the final ACK. This leads to the server keeping the resources allocated blocked until a timeout is reached. Depending on the servers' configuration, the allocated resources may make up a considerable proportion of the resources available and the timeout may be excessively long. If this attack is combined with a distributed approach, or if many SYN requests are started in parallel, the result is a DoS.

B. Imbalance of actors

Techniques for malicious actors to circumvent the legitimate control and regulation of data are publicly available and used. Legitimate actors, by contrast, cannot demand more bandwidth or privileged access from ISPs to create a power balance between themselves and sophisticated attackers. In fact, even direct responses to an ongoing attack may be problematic as in many cases attribution has to be examined and verified by juridical institutions to make any actions against the source legitimate. Legitimate actions therefore often focus on re-routing mechanisms or involve large redundancy set-ups to cope with outages. However, these fail-safe environments are necessarily limited and bound to the number of fall-back components integrated.

Currently, net neutrality places still further constraints on the technical capabilities of legitimate cyber actors. When considered strictly, net neutrality principles prevent live monitoring of suspicious traffic and hinder any attempts of attribution through the ISP, even though the ISP is often the first to notice unusual cyber activities. Traffic blocking is also against net neutrality standards, even if it is obvious to the technical expert that the traffic is involved in an ongoing attack. To resolve this issue, ISPs have begun to attempt to contact the initiators of such traffic; a tedious, costly and potentially fruitless venture.[36]

35 Lily Hay Newman, 'Github survived the biggest DDoS attack ever recorded', *Wired Security*, March 3, 2018, https://www.wired.com/story/github-ddos-memcached/, last access: March 16, 2018.

36 Michael Kan, 'Amid cyberattacks, ISPs try to clean up the Internet', *CSO Online*, February 23, 2017, https://www.csoonline.com/article/3173274/security/amid-cyberattacks-isps-try-to-clean-up-the-Internet.html, last access: January 7, 2018.

Discussing net neutrality in terms of traffic management and control inevitably leads to the insight that net neutrality protects both ordinary users and actors with hostile intent. While the rights and protection of innocent users should not be reduced unnecessarily, methods should be developed to empower legitimate over malicious actors.

C. Cyber Actions

The effects net neutrality has on cyber warfare scenarios can be divided into three distinct categories, based on the type of cyber action: cyber defence, proactive cyber defence and offensive cyber operations.

While cyber defence generally describes actions taken in the aftermath of cyber attacks and passive methods to deter or prevent the attack, proactive cyber defence allows an active response during and, to a degree, prior to cyber attacks taking place. Offensive cyber operations may range from aggressive, conflict-initiating operations, to supportive actions among allies during defensive cyber scenarios, but are generally directed against the attacker or its associated components.

Long-term defensive measures include log analysis, system hardening, redesigning of networks, training of personnel and developing incident response strategies. Immediate defensive techniques are especially those that are used to prevent further damage and neutralise the ongoing attack by measures taken at the victim's end only. Typical examples are the shutdown of servers, network components or infected devices and the blocking of traffic and services associated with the attack. These methods generally do not conflict with net neutrality principles if coordinated through legitimate law enforcement units or if immediate action is needed to prevent further damage to the ISP. However, immediate action through cyber units or proactive approaches through ISPs to prevent damage in foreign networks are currently limited.

One possible resolution of this conflict of interest would be that legitimate actors should be limited to defensive techniques to minimise contravention of net neutrality principles. However, purely defensive techniques are often of limited utility if the attacker's motivation is to cause the unavailability of services or devices. This is commonly seen in the various forms of denial-of-service attacks (DDoS). Furthermore, defensive strategies may also be considered too insecure if more sophisticated attacks are expected that may remain unnoticed for longer periods of time. These types of attacks are typically associated with espionage or information warfare, and it is these cyber activities in particular that are protected by current net neutrality standards. Although ISPs may be able to deduce that traffic is suspicious based on heuristics (i.e. without violating net neutrality), net neutrality would prevent further investigation

and action against the initiator unless authorised by law enforcement and judicial authorities.

Proactive cyber defence allows defensive methods to be combined with more aggressive monitoring and filtering rules. The line between defence and proactive defence is often blurred and depends on the specific technologies used. Firewall rules may be proactive and not compatible with net neutrality standards and DPI, which allows analysis on the content of the data packet passing and is often used to enforce Internet censorship. DPI is not compatible with net neutrality principles when applied to certain packets only.

Offensive cyber actions may vary greatly depending on the assets and technologies used. Any type of offensive strategy that aims at limiting, blocking, monitoring or manipulating specific traffic has to be considered as violating net neutrality principles. Whether legitimation can be given and under which circumstances has to be considered by the judiciary. It appears questionable whether it can be demanded of ISPs that they participate in military or governmental operations violating agreed telecommunication standards, such as net neutrality. But if they do not, this would imply a need for legitimate cyber actors to reroute traffic to their own network components to bypass ISPs in the context of offensive cyber activities to avoid limitations introduced by those ISPs during the operation.

If applied strictly to all traffic, demanding and enforcing the equal treatment of all data packets would prohibit the use of several cyber defence techniques. Those considered proactive would be particularly affected, since they rely on traffic being monitored based on origin, destination or content. If carried out by ISPs, these measures are not in line with net neutrality principles. Offensive cyber actions too may need the permission or active involvement of ISPs, which raises questions of legitimacy, particularly if this includes violations of agreed telecommunication standards.

D. Cyber Power

Actors in cyberspace are represented by their data and traffic. Controlling either data or traffic corresponds to controlling the actor. Limiting the capabilities of legitimate actors to legally interfere with malicious traffic is a digital form of unilateral disarmament, and as a consequence has the capability to destabilise cyber sovereignty.

As described above, net neutrality places limits on the whole range of legitimate actions in cyberspace, reducing both offensive and preventive measures. However, these limitations again only apply to actors bound by restrictions, while illegitimate actors can choose to circumvent or disregard them. The limitation of preventive measures plays a major role not only in constraining defence against future attacks,

but also in helping attackers conceal their activities and avoid prosecution. This is because net neutrality prevents ISPs from collecting only selected data from the traffic they forward. Paradoxically, this has often been a contributory factor to the adoption of general telecommunications data retention (e.g. in Germany). The irony is that from the point of view of net neutrality, if you collect data on everybody this is legal and acceptable, but only collecting data on traffic that appears suspicious is not.

Overall, strict application of net neutrality principles contributes to an unbalanced cyberspace. Legitimate actors are being deprived of rights granted in non-digital circumstances, while the community is unable technically to enforce net neutrality on the attackers' side as well. This gives rise to a substantial mismatch in the distribution of cyber power among actors.

4. OPPORTUNITIES AND CHALLENGES

If net neutrality principles are weakened, ISPs will need to reserve bandwidth and develop reliable methods to identify privileged customers and services without introducing additional physical media in order to guarantee high transmission rates for these customers and services; the mere throttling of 'unprivileged traffic' is insufficient. It is likely that both channelling and protocol developments will take place. Additional hardening of access to these channels may help to ensure that only legitimate users have access to the channel. Creating privileged channels contributes to restoring a balance between legitimate cyber actors and attackers in cyberspace. Currently, attackers have the ability to simply allocate bandwidth and to technically enforce prioritised processing, while the options of legitimate actors are severely limited.

Cyber defence support among allies could be affected positively by weakening net neutrality principles and installing prioritised channels. Establishing privileged high-speed connections may prove valuable in scenarios where remote access to networks under attack is needed. This occurs when network administration personnel are faced with sophisticated cyber attacks for which they are insufficiently prepared. In such cases, remote access could be established, even in scenarios including a denial of service, by technically enforcing processing of data received by the prioritised channels through networking rules and interrupt handling strategies. Such methods could be implemented easily in Software Defined Networks (SDNs), however, standards should be defined that ensure these measures conform to our democratic norms. This would in turn not only allow remote support during cyber incidents but facilitate forensic activities during and after the attack.

Prioritised channels could also be used to uphold a minimal service availability if, for example, critical infrastructure is being targeted. The use of prioritised channels allows the separation of critical traffic from common or public traffic. While a smaller number of sophisticated attacks should be expected to target the prioritised channels, the larger portion of less sophisticated and limited attacks will target the public traffic channels, which in turn may be processed on less prioritised components with limited device access. Although this may appear unfair at first, current security standards attempt to enforce precisely this by network virtualisation and service encapsulation. However, due to their high abstraction layer, several vulnerabilities arise within solutions based on virtualisation and the attack surface is even enlarged.[37] These vulnerabilities are not to be expected on lower abstraction layers, which is why we would envision low layer solutions.

Although several benefits could be expected from weakening net neutrality principles and establishing prioritised traffic through ISPs, new attack vectors must also be expected. As bandwidth and transmission rates are high-value assets in cyberspace, attackers are likely to work on ways to obtain access to prioritised traffic. Therefore, the development of such technologies and the definition of adequate standards should not be left to the free market only. It must also be guaranteed that democratic values and standards are not being undermined. However, this is an obligation of Western democracies that should not only apply for legitimate actors, but must also be enforced for malicious actors threatening the cyber domain.

5. OUTLOOK

This article has explored net neutrality and networking principles from both strategic and technical views. The handling of net neutrality and traffic equality within the EU, UK and Russia were compared and discussed. Particular attention was given to the influence the different approaches have in the uprising congested and contested cyber domains as expected in cyber warfare scenarios.

Russia's distinct approach to net neutrality and network regulations in general was explored, highlighting the measurements taken and scheduled to prevent the destabilising effect net neutrality has on cyber power and sovereignty. While several of the technologies and regulations established within Russia are not acceptable by Western standards due to their limitation of individual rights, the deployed methods show Russia's sensibility to the arising threats and an awareness of the cyber power imbalance.

37 Candid Wueest, 'Threats to virtual environments', *Symantec Security Response*, August 12, 2014; European Union Agency for Network and Information Security (ENISA), *Security aspects of virtualization*, February 2017, ISBN 978-92-9204-211-0.

The EU is currently struggling with enforcement of the approved Regulation on the telecommunications single market. The Regulation allows national judicial interpretation which leads to different implementations of net neutrality within the EU. This condition is unsatisfactory as it creates an imbalance between EU members both in terms of market regulations and cyber power. This limits joint cyber operations, as cyberspace is not limited by national borders, but data traffic is treated according to national jurisdiction, possibly hindering prosecution depending on the national networking regulations.

The UK has made a step forward in terms of providing broadband access to all consumers, however, it has also been considered as one of the 'enemies of the Internet' by the RSF since 2014. The UK is known for its surveillance capabilities, which can also be applied through local ISPs. It is noteworthy that the UK plays a major role in building the transatlantic backbone of the Internet, especially between the United States and EU. Severe limitations of net neutrality must be expected to follow the withdrawal of the UK from the EU unless regulatory and technical enforcement are developed.

Discussions on net neutrality are discussions on traffic management. There is a requirement to define standards and policies that regulate when and how legitimate actors may demand assistance by ISPs to either prioritise their own traffic or limit the traffic of potentially malicious actors. As blocking or reducing malicious traffic may result in unjust penalisation of unaware end-users, this paper advocates the prioritisation of governmental (or governmentally legitimated) cyber actors. The aim of any legitimate action in cyberspace must be to protect civilian users while defending networks and services and to establish cyber sovereignty and power.

While there are good reasons to weaken net neutrality principles, this should be done in a controlled manner and monitored by independent authorities. As demonstrated in the case of the United States both before and immediately following the 2017 easing of net neutrality constraints, uncontrolled outsourcing to private companies bears the risk of abusive methods that not only influence the end users of telecommunication services but may also limit free market growth and lead to monopolies.

Net neutrality regulations should consider the protection of individual rights and equality among civilian end-users but must also ensure stability in cyberspace and equality among actors. This is of particular importance in cyber war scenarios where some states are less constrained in their legitimate cyber activities than others. There are two possible choices: either to technically enforce net neutrality (which has already been proven impractical in the face of botnets or distributed cyber attacks as the attribution of cyber actions remains an unsolved task) or to define regulations that

allow legitimate actors to rebalance cyber power and regain control over congested networks during cyber incidents to uphold sovereignty in cyberspace.

AKNOWLEDGEMENT

The authors are grateful for research assistance from Lincoln Pigman in the preparation of this paper.