Unlearned Lessons from the First Cybered Conflict Decade – BGP Hijacks Continue

Prof. Yuval Shavitt
Dr. Chris C. Demchak

INTRODUCTION

Unlearned lessons are those where the harm, attack methods, or malicious tools are demonstrated publicly and yet neglected by those who need to respond or better plan for future attacks. By 2010, reports of network traffic hijack attacks – called here Internet Protocol (IP) or Border Gateway Protocol (BGP) hijacks – had already surfaced. Most notably publicized was the China Telecom IP hijack attack in that year where 15% of the global Internet traffic was rerouted or "hijacked" through servers in China.[1] While the scale of this original event has been debated, there is little doubt that throughout the following decade, attacks of this kind continued. Eight years later, in 2018, we reported on China Telecom using its otherwise seemingly innocent network servers to reroute (or hijack) Internet traffic through China at its will. At the time, the company had 10 "points of presence" (PoPs, locations where a company's routing equipment is located) in North America, each strategically located and available to hijack or divert network traffic through China from North America.[2] The 2018 paper drew significant attention to the problem by the general public (through popular media outlets), the cybersecurity and research communities, and various stakeholders in western nations' governments, and yet the lesson is still unlearned by many of the same nations currently being victimized by China Telecom illicit activity and other BGP hijacks.

This essay discusses what has changed in the few years since the 2018 paper was published. Several interesting developments occurred in the last decade that suggest awareness is increasing but that the lessons are being learned too slowly and are still too fragmented across nations. Three years later, in 2021, we can report that China Telecom is still hijacking traffic using its global presence in Europe, Asia, and Africa. Major developments over the decade include three major observations.

All ideas stated here are solely those of the author(s) and do not reflect the positions or policies of any element of the U.S. Government.

Prof. Yuval Shavitt is Professor of Electrical Engineering at Tel Aviv University. Before joining Tel Aviv University, he worked for four years at the Networking Center of Bell Labs, Holmdel, NJ. He has published seminal papers in the fields of caching, routing, IP hijack attacks, and network measurements. In 2004, he founded the DIMES project for mapping the Internet infrastructure using thousands of lightweight software agents, which revolutionized the field of Internet measurement and mapping. Data gathered by DIMES was used by academicians worldwide. In 2014 he established BGProtect, a company that uses the DIMES approach to protect nations and large organizations against IP hijack attacks and provide network infrastructure threat intelligence.

1. Despite increased awareness of network operators and the networking research community regarding the risks of IP hijack attacks, the levels of adoption of means to make IP hijack attacks harder to carry out are still insufficient to declare this lesson learned.
2. The scale of the unfettered global expansion of large Chinese Internet service providers has made IP hijack execution somewhat easier and IP hijack detection harder worldwide.
3. Largely in North America and a narrow set of allies, an increased awareness among policymakers and other national leaders about Chinese-linked BGP attacks has led to enhanced efforts to use regulation to limit the use of Chinese telecommunication equipment and activities in critical national infrastructure, but many other states still welcome the overly generous and seemingly innocuous low-bids by Chinese vendors.

And the ‘game’ is still afoot. While the 2018 paper provides more detail on how the BGP hijacks occurred, it is helpful to reiterate a few details. The Internet is a global system of interconnected computer networks that push data to each other. Continuously, millions of streams of Internet traffic are guided from one node of a network through another and another, each possibly part of a different network, to the final destination node indicated by the published Border Gateway Protocol (BGP) routing tables. These intervening networks are, for routing purposes, called “autonomous systems” (AS) and are given unique numbers (AS Numbers, or ASNs) that are used to build the global BGP routing table. The tables themselves are constructed by the ASs self-reporting on what nodes they connect. During regular routing of Internet traffic, each AS announces its readiness to receive traffic and passes it along to neighbors by posting that information in BGP. With this information, the networks that are part of the Internet build their routing tables, which are used

With degrees in engineering, economics, and comparative complex organization systems/political science, **Dr. Chris C. Demchak** is Grace Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber Innovation Policy Institute, U.S. Naval War College. In publications and current research on cyberspace as a global, insecure, complex, conflict-prone "substrate," Dr. Demchak takes a socio-technical-economic systems approach to comparative institutional evolution with emerging technologies, adversaries' cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and regional/national/enterprise-wide resilience against complex systems surprise. Her manuscripts in progress are "Cyber Westphalia: States, Great Systems Conflict, and Collective Resilience" and "Cyber Commands: Organizing for Cybered Great Systems Conflict."

by each AS to send traffic from its internal customers on to others – in short, to anyone. IP hijack attacks are attacks where Internet traffic between the original sender and the destination is forced to travel along a set of intervening networks and nodes that include nefarious networks making copies of or alterations to the transiting Internet packets.

It is in the buried and often technical details of routing lists of ASs and transmission times that one finds small deviations or, changes in routes for nonaccidental periods of time. These deviations are often buried in the routes so that inattentive senders or recipients are not alerted. The traffic may arrive at its final destination a bit delayed, but in the meantime, it has been pushed unnecessarily through other nodes capable of making a quick copy of everything that transits through their location. Since the traffic eventually is received, it is and has been easy for either party (sender or receiver) or their network operators, to notice that critical information meant only for selected parties may be accumulating in someone else's database for decryption and use later.

For example, Figure 1 depicts routes from a recent deflection event in Europe. For about 10 minutes, traffic from hundreds of small networks worldwide (but mostly in Europe) was routed to COLT Telecommunications in West Europe via the TransTelecom's PoP in Moscow, Russia. TransTelecom was used by COLT to accept traffic from Russia and Central Asia. During the deflection event, COLT routes that were announced by TransTelecom were picked up by Russian Akado Telecom (previously known as Comcor) from Inetcom, a local Moscow provider. Akado Telecom then announced the routes to its many peers and, as a result, worldwide traffic (mostly from W. Europe) started traversing Moscow. The number of networks routing through TransTelecom during this deflection event increased sevenfold. The fact that only small networks were affected by this deflection is unusual. This oddity suggested that larger networks, which would be more visible in the BGP monitoring tools, were not receiving these route announcements on purpose. The game can be quite subtle if the adversary is trying to operate unnoticed.

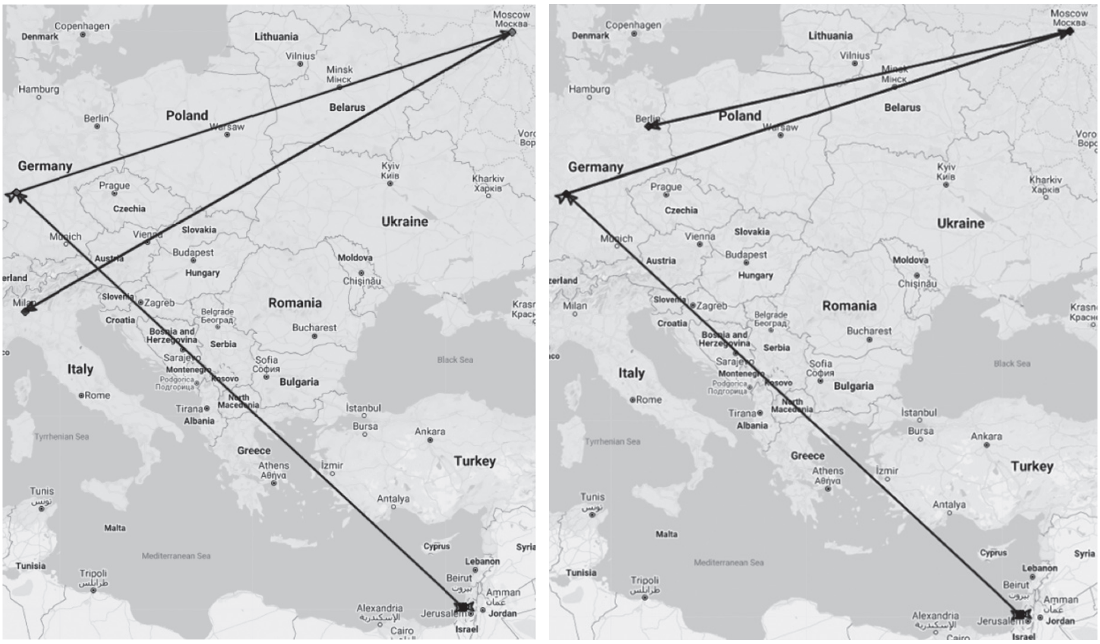

Figure 1: Two route examples from a 10-minute deflection of traffic towards COLT networks in West Europe via Moscow. The event occurred on March 7th, 2021, and affected traffic from hundreds of small networks around the world.

The Technology Sector Wakes Up – but Lessons Learned Lag Behind

By the late 2010s, there was increased awareness among network operators and the networking research community at risk about possible IP hijack attacks. The increase in the number of IP hijack attacks made “BGP hijack” a more familiar term that had emerged from obscurity to be known among technologists. In a survey conducted in 2017 among 75 network operators, over 90% of the surveyed operators claimed to be knowledgeable about BGP hijacking and how it happens. Yet, 41% reported that their organization had been a victim of a BGP hijack attack, and over half of the attacks lasted longer than an hour. A quarter lasted longer than a day, enabling a considerable amount of data to pass through unintended nodes in networks.[3]

As a result, there was also a reported increase in the adoption of means to make IP hijack attacks at least harder to carry out. The greater awareness of hijacking events led also to greater adoption of some operation norms by Internet service providers (ISPs). Until recently, one common way to hijack Internet traffic and reroute it to a block of IP addresses (an Address Prefix, or AP) was for the hijacking AS (Autonomous System or node in the network) to announce ownership of a particular AP using BGP. Since BGP was originally designed with no underlying security concerns, there is no intrinsic way in BGP to prevent any network on the Internet from announcing ownership of any AP regardless of its real owner. Over the years, large ISPs had adopted various means to verify that their customer networks do not announce APs that they are not allowed to announce. This verification, however, is not standardized and has been implemented inconsistently among network providers.

Some solutions have emerged but are still not consistently employed or standardized in processes or regulations. One promising standard – the Resource Public Key Infrastructure (RPKI), also known as Resource Certification, designed by the Internet Engineering Task Force (IETF) earlier on and available by 2011, was intended to solve the AP ownership verification, or in RPKI jargon, the Route Origin Authorization(ROA) in a standard way.[4] When using this standard, a distributed database allows each AP owner to communicate who is allowed to announce its address space. Since AP announcements carry the entire path to the AP, one can easily verify that the intended AS (namely the destination network) at the end of the route is legitimate.

Nonetheless, RPKI adoption has been irritatingly slow for most of the past decade. Momentum picked up significantly around 2017,[5] but recent statistics by the U.S. National Institute of Standards and Technology (NIST) show that only about one-third of the APs have valid RPKI entries.[6] Indeed, recent reports demonstrate that using RPKI improves the filtering of invalid route announcements.[7] However, it should be noted that RPKI protects against only one type of hijack attack (origin attacks), and it is not a comprehensive solution to the general problem of IP hijack attacks, not even to BGP hijack attacks.

A similar tale can be told about the MANRS (Mutually Agreed Norms for Routing Security). It is another initiative that calls for ISPs and Internet exchange points (IXPs) to declare that they follow a certain set of actions to improve routing security. This includes announcement filtering (e.g., by using RPKI), maintaining ROA information up to date, and even publishing contact information to promote communication and collaboration between network operators. The number of organizations that declare adherence to MANRS has also increased recently and steadily, but not sufficiently.[8]

Technological awareness has not yet led to lessons being learned universally. One lesson has escaped the networking community and decision makers, even after the demonstrations of 2010 and afterward. Furthermore, the complexity of BGP continues to make it difficult to detect hijacks. For a variety of spontaneous reasons, route selection is sometimes hard to predict and varies without malicious intent. The easiest way to determine how to exploit BGP and get traffic to go through some otherwise unintended AS node en route is for a state or a criminal organization to have an otherwise legitimate node along major routes – a Point of Presence (PoP) located in a routing facility at key network intersections points in the global Internet. By these bad actors' masking as a legitimate node in the network, it is very difficult for other network elements to identify a nefarious node.

China Network Explosion – Hiding in Plain Sight

The global expansion of large Chinese ISPs into the backbones of national networks across the world makes IP hijack operations easier to conduct, and also makes IP hijack detection more difficult due to the scale and omnipresence of these providers. The number of Chinese PoPs in major locations around the world, especially outside of established democracies, has been steadily increasing. Two Chinese telecommunications providers in particular, China Telecom (CT) and China Mobile International (CMI), have significantly expanded their networks in the past decade. Both are now significant players in the global non-Chinese Internet traffic transit market, with extraordinary access to – and ability to divert – routine network traffic of major and minor nations globally, especially in recent years.

To evaluate Chinese providers presence in the global transit market, the Internet transit market was mapped over the last decade for important countries in Africa (South Africa, Nigeria, Uganda) and South America (Brazil, Argentina, Chile). In addition, a few small nations in Europe and Asia (Singapore, Israel, Finland) were also considered. Until 2018, these countries did not have a significant portion of their traffic routed via a Chinese transit provider. In June 2019, however, Brazil started seeing a sudden and, for this industry, quite large increase in Brazilian traffic carried by CMI out to the rest of the world, jumping from 0.5% to about 6% (see Figure 2). The majority of this increase came from Oi S.A. (previously known as Telemar, a large Brazilian telecommunications company), which started using CMI as the major upstream provider. As a major rising nation with considerable natural resources and population, the communications of political, government, commercial, and civic leaders of Brazil would be of considerable interest to the Chinese government.

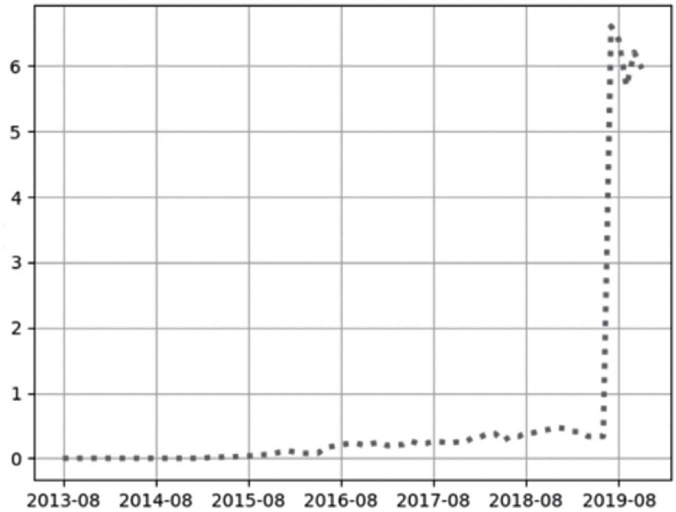

Figure 2: The Sudden 6-fold rise of China Mobile as a percentage of the Brazilian foreign transit market.

Across the sea but also in an area of considerable vast natural resources, Africa looms large in the global strategic influence and control agenda of China's state and commercial leaders.[9] In August 2019, several African nations increased the use of China Telecom as a provider, especially in Angola and South Africa (but also Nigeria, Namibia, and Kenya). At the same time, curiously, Russian TransTelecom – a peer of CT – started 'announcing' (via BGP) many African prefixes that it received from CT. As a result, a significant portion of the traffic of about 350 Address Prefixes (APs), mostly in Africa, started flowing through TransTelecom to and through China Telecom's PoP in Moscow even though intended for quite distant destinations. Nothing in the colloquial understanding of the Internet's design, which intended for data to travel by the shortest routes, would send traffic from South Africa to Israel through Moscow instead of through a major hub in western Europe, as shown in Figure 3. Once or twice, it could be a result of a mistake (a route leak) at TransTelecom or a change in the policy due to other political or economic reasons. However, TransTelecom and CT claim to be working together to shorten routes from China to West Europe.[10] It is not clear why TransTelecom would announce China Telecom routes to many peers in Europe in any case. That arrangement opens considerable opportunities for nefarious hijacking campaigns already well-demonstrated by China Telecom and its peer partner in Russia, TransTelecom.

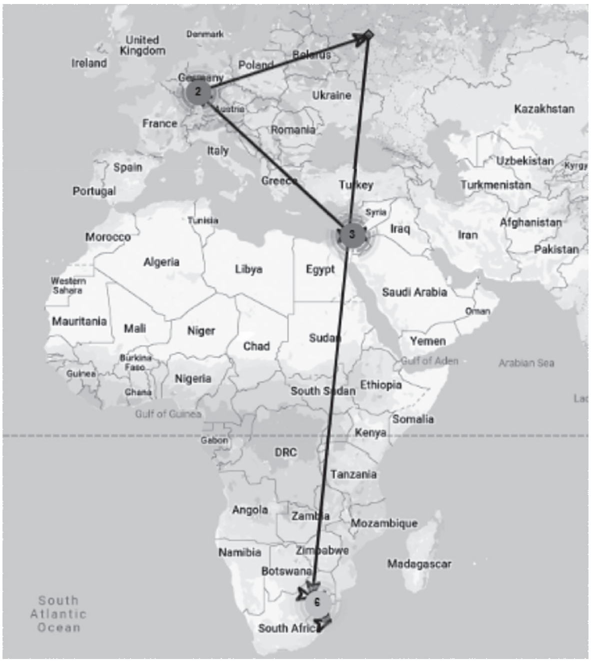

Figure 3: An example of a deflection through Moscow by TransTelecom and China Telecom. Routes between Israel and South Africa normally route through Internet exchange points in London or Frankfurt, where traffic is handed to African local or regional carriers that uses a submarine cable to transport traffic to Africa.

In the complex world of networks underpinning societies, bad faith players with a myriad of legitimate business footholds around the world are increasingly difficult to monitor, expose, and ultimately to get the political will to expel from the global transit market. Figure 4 demonstrates extraordinary increases in the transit traffic handled by CT in just one AP at the Africa nation – Zambia. Overnight, the portion of traffic towards this AP that is carried by CT grew from 0 to about 60% and a day later to about 85%. Namely, almost all the traffic to this and other APs in Zambia traversed the CT network. It is perhaps not coincidental that Zambia is also one of the nations whose government is being provided facial recognition technology by a Chinese vendor as well.[11] This increased Chinese penetration in the global transit market will challenge – and is likely to dampen the ability of – services that attempt to alert others against IP hijack attacks in real-time. Until recently, Chinese providers were not significant players in the global transit market, and it was relatively easy to identify hijacked routes based on (and we are oversimplifying here) the bare presence of a Chinese provider close to a local Western provider. With the integration of Chinese providers in the global transit market, considerably more and deeper analysis is needed to distinguish between legitimate routing through Chinese providers and malicious hijack attacks. Only recently have initial steps to use deep learning for this challenging task been published and the use of artificial intelligence (AI) for detecting such bad faith behavior is still nascent.[12] The response has been at best muted in the capitals of even Western democracies.

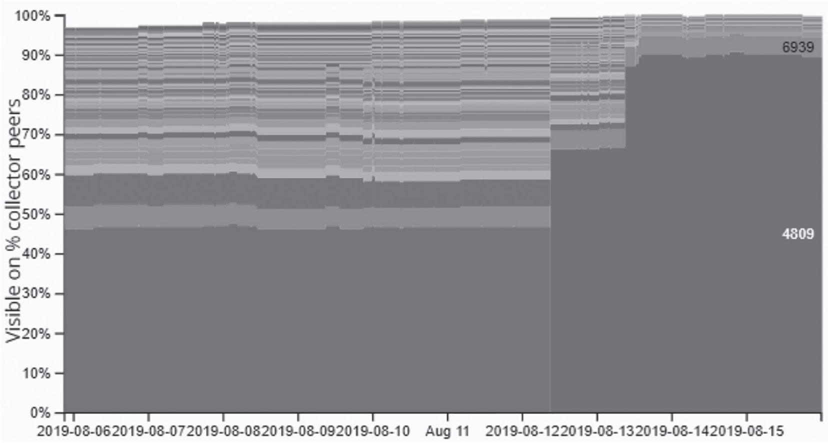

Figure 4: An example of the increase of traffic served by China Telecom (AS 4089) for an IP address block in Zambia during August 2019. CT share grew suddenly from zero to 60-85% for the rest of the month of August. This situation continued for several months.

The graph was generated using the RIPEstat site (stat.ripe.net).

Political Awareness Spotty – Action Resisted

If the technologists did not act to forestall an IP hijack despite evidence of the rise of Chinese telecommunications providers globally, political leaders of most nations were, and have been, even slower to react. Political and administrative communities in most established democracies rarely have any technical training or in-depth understanding of cyber threats to their networked infrastructures. When technical advisors are unable or unwilling to perceive the threats in the insecurity of the BGP global system, those they advise in political administrations will be commensurately even less responsive.

For the first six years of the 2010's decade, hijacking attacks were not dealt with publicly by Western democracies. Only in 2017, with the new US administration's generalized hostility to China, did attention to the cyber threat of network hijacks begin to have a toehold in the political debate about national security and the rise of a hostile peer power. By late 2018, in North America, our work on China Telecom BGP hijacking joined other reports about the undesirable behaviors of Chinese state champions, and the conversation about BGP hijacking moved from politically invisible to being perceived as a component of the general rise in cyber conflict – labeled here as "Great Systems Conflict" – with China.[13]

By early 2020, the Trump administration's actions against Chinese information technology corporations (many via Executive Orders) had finally spread to China Telecom – the central actor in the BGP hijacking noted in our late 2018 article.[14] A 2020 report[15] by the Senate Committee on Homeland Security and Governmental Affairs cited our previous work. In late 2020, the U.S. Federal Communications Commission (FCC) announced that it had begun a process of restricting China Telecom from operations in the US.[16] Six months later, in June of 2021, and under a new administration, the FCC announced it was imposing additional restrictions on US companies buying and installing telecommunications equipment from China.[17]

In Canada, in late 2018, the Prime Minister's national security adviser said that Canada would raise the traffic hijacking issue with senior Chinese officials at a security and legal affairs meeting in Beijing at the end of that year.[18] In February 2019, the Canada Parliament Standing Committee on Public Safety and National Security held a meeting that discussed the security risk from Chinese ISPs operating in Canada and the usage of Chinese-made telecommunication equipment in Canada's critical infrastructure.[19] Prof. Shavitt, one of the coauthors, was one of the two experts that testified in that meeting. Although Canada is acting to restrict Chinese firms in its telecommunications sector, it is resolutely moving much more discretely.[20]

Outside of North America, the political actors' awareness in established democracies of the ease and increasing threat from state-sponsored BGP hijacks has led to limited actions largely focused on one adversary – China. While all the 'Five Eyes' (i.e., Australia, New Zealand, UK, US, and more recently Canada) have taken steps to reduce their dependence on Chinese companies and telecom equipment, only recently has the biggest other actor (or bloc of established democracies) – the European Union (EU) – been willing to identify the potential for telecommunications misbehavior on the part of the Chinese specifically, let alone Russia, Iran, and others.

At the end of 2020, the EU and China signed an EU-wide bilateral investment deal – which every EU country has on its own with China save Ireland – in which China promised to allow EU companies into its home telecommunications market and ban forced technology transfers.[21] EU negotiating leaders signed the deal after over seven years of negotiations despite the known tendency of the Chinese government to make promises it does not keep on the ground, such as its original WTO admission agreement, and despite the clear evidence of a late-day quiet insertion by China of language enabling it to punish EU countries that decide to ban Chinese telecommunications companies Huawei or ZTE from their networks.[22] The efforts to ratify this trade agreement have currently been suspended. Other EU telecommunications-related restrictions, guidelines, and scrutiny on foreign vendors – especially on Chinese firms – have focused specifically on 5G equipment,[23] subsidies,[24] foreign direct investments screening[25] and takeovers or mergers,[26] and on guarding against economic competition and dependency from Chinese suppliers in strategic areas.

Missing from these actions is the nefarious use of otherwise normal traffic routes across all EU networks. Beyond that, there is little evidence of awareness of BGP hijacking attacks, no action, and no specific attention to Chinese telecommunications companies in this form of network attacks, even though it is known to the technologists across the EU. The problem cannot be solved by a nation here and a nation there if the wider global net is increasingly populated with PoPs and equipment owned and operated by states willing to act in bad faith.

CONCLUSION

This problem is not going to resolve itself in any way favorable to democracies unless their leaders and technologists acknowledge the evidence already abundantly present of an existential threat to the integrity of the Internet itself. It does not matter how strongly encrypted a data stream being shared across nations is if an adversary state or its proxies can routinely capture a copy of it and decrypt it at their leisure. As we noted in our 2018 piece, if legitimate and acceptable behavior cannot be assured, the footholds of the bad faith actor need to be expelled. Ironically, the Chinese government does not allow any foreign PoPs within China, indicating at least one nation where the lesson of BGP hijacking has been learned precisely because that nation knows what can be perpetrated. We suggested then, and repropose now, a policy of “Access Reciprocity” in which PoP presence by Chinese companies is matched, node for node and free presence for free presence, with overwatch and expulsion rules. The intent is to induce sufficient dedicated political and technical attention at the highest and lowest levels for a better balance between democratic and authoritarian information technology systems.[27]

Just before the final version of this article was ready to print, the FCC announced it will revoke China Telecom America's license to operate in the US.[28] This is certainly the outcome we were suggesting in this and our previous publication in 2018. However, that loss of license only affects CT's operations inside the US, not the wider operations or traffic hijacking by CT Global across any routes not transiting the US. Nor does it stop CT from using other services to carry its hijacked traffic as their own across the US en route to China or back to the original legitimate destination.

The great unlearned lesson of BGP hijacking is precisely that basic reciprocal fairness cannot be assumed unless it is ensured by fair and transparent processes that the bad faith actor cannot subvert. In an asocial global environment, having such a policy could be, as Robert Axelrod once noted, clarifying and effective in forcing hostile states to the table to cooperate on at least this one major threat.[29] Such an outcome is immensely desirable, but the window of opportunity to achieve it is quickly closing with the broadening and deepening presence of authoritarian state networks throughout the globe. It is time to learn this essential lesson and move to action. The US has made the first step in acting against this bad behavior by a state champion of China. We hope that Canada and other allies will follow suit.

NOTES

1. https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes/.
2. Chris C. Demchak and Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs Journal* 3, no. 1 (October 21 2018), https://scholarcommons.usf.edu/mca/vol3/iss1/7/.
3. P. Sermpezis, V. Kotronis, A. Dainotti, and X. Dimitropoulos, 2018, A Survey among Network Operators on BGP Prefix Hijacking". ACM SIGCOMM Computer Communication Review (CCR) 48(1):64–69, Jan 2018.
4. Geoff Huston and Randy Bush. 2011. "Securing BGP and SIDR". IETFJournal7, 1 (2011).
5. Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, H. Shulman, "Are We There Yet? On RPKI's Deployment and Security, NDSS, 2017.
6. https://rpki-monitor.antd.nist.gov/.
7. Cecilia Testart, Philipp Richter, Alistair King, Alberto Dainotti, and David Clark. "o Filter or Not to Filter: Measuring the Benefits of Registering in the RPKI Today", Passive and Active Measurement (PAM) 2020, pp 71-87
8. Cristian Hesselman et al., "A responsible internet to increase trust in the digital world," *Journal of Network and Systems Management* 28, no. 4 (2020).
9. Celine Sui, "China-Africa Economic Relationship," *Courting Africa: Asian Powers and the New Scramble for the Continent* (2020).
10. https://company.ttk.ru/page4219071.html#!/tproduct/142079272-1520861032521.
11. Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents - Employees embedded with cybersecurity forces in Uganda and Zambia intercepted encrypted communications and used cell data to track opponents, according to a *Wall Street Journal* investigation," *Wall Street Journal,* August 15 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.
12. Tal Shapira and Yuval Shavitt. A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding. ACM SIGCOMM 2020 Workshop on Network Meets AI & ML (NetAI 2020), August 2020.
13. https://cyberdefensereview.army.mil/Portals/6/Documents/2021_spring_cdr/COVID_CDR_V6N2_Spring_2021_r4.pdf.
14. https://www.washingtonpost.com/national-security/trump-administration-moves-against-chinese-telecom-firms-citing-national-security/2020/04/10/33532492-7b24-11ea-9bee-c5bf9d2e3288_story.html.
15. https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.
16. https://www.reuters.com/article/usa-china-tech/fcc-begins-process-of-halting-china-telecom-u-s-operations-idUSKBN28K2ER.
17. https://www.nytimes.com/2021/06/17/technology/fcc-china-technology-restrictions.html.
18. https://www.theglobeandmail.com/politics/article-china-telecom-hijacked-internet-traffic-in-us-and-canada-report/.
19. https://www.ourcommons.ca/DocumentViewer/en/42-1/secu/meeting-149/evidence.
20. David Ljunggren, "Canada has effectively moved to block China's Huawei from 5G, but can't say so," *Reuters*, August 25 2020, https://www.reuters.com/article/us-canada-huawei-analysis/canada-has-effectively-moved-to-block-chinas-huawei-from-5g-but-cant-say-so-idUSKBN25L26S.
21. https://thediplomat.com/2021/01/the-pitfalls-of-the-china-eu-comprehensive-agreement-on-investment/.
22. https://www.scmp.com/economy/china-economy/article/3116896/china-tried-punish-european-states-huawei-bans-adding.
23. https://www.euractiv.com/section/digital/news/eu-countries-keep-different-approaches-to-huawei-on-5g-rollout/.
24. https://www.bloomberg.com/news/articles/2021-04-27/eu-threatens-fines-and-merger-bans-for-chinese-state-firms.
25. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200924_Chinese_Tech.pdf.
26. https://fortune.com/2021/05/05/eu-china-europe-restrictions-foreign-takeovers-investments-margrethe-vestager/
27. Demchak and Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking."

NOTES

28. Simon Sharwood, "China Telecom booted out of USA as Feds worry it could disrupt or spy on local networks - FCC urges more action against Huawei and DJI, too," The Register, October 27 2021, https://www.theregister.com/2021/10/27/china_telecom_booted_out_of/.
29. Robert Axelrod and William Donald Hamilton, "The evolution of cooperation," *science* 211, no. 4489 (1981).