UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

Institut mezinárodních studií

Bakalářská práce

2024 **Huyen Ngoc Dinhová**

UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

Institut mezinárodních studií

Analýza politiky Donalda Trumpa vůči čínské společnosti Huawei a role kybernetické bezpečnosti

Bakalářská práce

Autorka práce: Huyen Ngoc Dinhová
Studijní program: Teritoriální studia
Vedoucí práce: Mgr. Jana Sehnálková, Ph.D.
Rok obhajoby: 2024

Prohlášení

1. Prohlašuji, že jsem předkládanou práci zpracovala samostatně a použila jen uvedené prameny a literaturu.
2. Prohlašuji, že práce nebyla využita k získání jiného titulu.
3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne 28.dubna 2024 Huyen Ngoc Dinhová

Bibliografický záznam

DINHOVÁ, Huyen Ngoc. *Analýza politiky Donalda Trumpa vůči čínské společnosti Huawei a role kybernetické bezpečnosti.* Praha, 2024. 53 s. Bakalářská práce (Bc). Univerzita Karlova, Fakulta sociálních věd, Institut mezinárodních studií. Vedoucí bakalářské práce Mgr. Jana Sehnálková, Ph.D.

Rozsah práce: 70 800 znaků

Abstrakt

Bakalářská práce se zabývá analýzou zahraniční politiky bývalého amerického prezidenta Donalda Trumpa vůči čínské společnosti Huawei. Cílem práce je prozkoumat, proč Trumpova administrativa rozhodla zakázat společnosti Huawei poskytovat 5G služby na americkém a celosvětovém trhu. Práce analyzuje faktory, které vedly k zákazu společnosti Huawei ze strany Trumpovy administrativy, a zaměřuje se na to, jak důležitá byla otázka kybernetické bezpečnosti při tomto rozhodování. Metoda *process tracing* je v této práci použita k systematickému zkoumání daných faktorů. Práce také pracuje s analýzou zahraniční politiky, která vychází z teorie ofenzivního realismu, jež zdůrazňuje důležitost udržení technologického vedení pro vojenskou a ekonomickou převahu USA. Zároveň bere v úvahu domácí a individuální faktory. Výsledky analýzy naznačují, že Trumpova administrativa zakázala Huawei jak kvůli obavám o národní bezpečnost – tedy jak kvůli obavám o kybernetickou bezpečnost, tak kvůli obavám o technologický růst Číny. Samotný Trump viděl kauzu Huawei jako nástroj k obchodního vyjednání a ukazuje se tedy transakční prezidentství Donalda Trumpa. Bakalářská práce přispívá k lepšímu porozumění vztahům mezi USA a Čínou, zejména v kontextu technologické konkurence a kybernetické bezpečnosti

Abstract

The present bachelor thesis presents the analysis of the foreign policy of former US President Donald Trump towards the Chinese company Huawei. The thesis aims to explore why the Trump administration decided to ban Huawei from providing 5G services in the US and global markets. The thesis analyses the factors that led to the Trump administration's ban on Huawei and focuses on how important the issue of cybersecurity was in this decision. The process tracing method is used in this thesis to systematically examine the factors in question. The thesis also employs a foreign policy analysis based on the theory of offensive realism, which emphasizes the importance of maintaining technological leadership for military and economic superiority. It also takes into account the domestic and individual factors. The results of the analysis suggest that the Trump administration banned Huawei because of national security concerns-that is, both cybersecurity concerns and concerns about China's technological growth. Trump himself saw the Huawei case as a bargaining tool for the upcoming election, thus showing the transactional presidency of Donald Trump. This bachelor's thesis contributes to a better understanding of U.S.-China relations, particularly in the context of technological competition and cybersecurity.

Klíčová slova

Kybernetická bezpečnost, USA, Čína, Huawei, analýza zahraniční politiky, process tracing, Donald Trump, technologické soupeření, 5G, americko-čínské vztahy

Keywords

Cybersecurity, USA, China, Huawei, foreign policy analysis, process tracing, Donald Trump, technological competiton, 5G, U.S.- China relations

Title

Analysis of Donald Trump´s Policy Towards Huawei and the Role of Cybersecurity

Poděkování

Chtěla bych poděkovat paní doktorce Sehnálkové za cenné připomínky a rady během konzultace. A mé poděkování také patří mém kamarádkám a mému příteli, kteří byli mou psychickou oporou po celou dobu mého studia.

Obsah

Úvod

V současné době realizujeme velkou část našich životů v online prostředí, známém také jako kyberprostor. Pokrok v informační a komunikační technologii vedl k rychlému a rozsáhlému rozšíření digitální ekonomiky, která sice umožnila rozvoj mezinárodního obchodu a investic, ale současně otevřela dveře novým hrozbám v podobě kybernetických útoků. Kybernetické útoky mají za cíl krást data, sledovat uživatele a provádět další nekalé činy. Vzhledem k těmto hrozbám se kybernetická bezpečnost stává neodmyslitelnou součástí národní bezpečnosti. S nástupem technologie 5G se tento problém umocňuje, neboť nová telekomunikační mobilní síť přináší nové výzvy v kybernetickém prostředí. Proto je nezbytné, aby vlády přijímaly kybernetická opatření k ochraně svých dat v 5G sítích.

Největším světovým výrobcem zařízení potřebných pro provoz nové sítě 5G je Huawei, původem z Číny. Řada zemí, především Spojené státy americké, vyjádřila znepokojení nad účastí společnosti Huawei při budování sítí páté generace, a to kvůli jejím možným vazbám na Komunistickou stranu Číny. Administrativa bývalého amerického prezidenta Donalda Trumpa přijala bezprecedentní opatření namířená proti čínské společnosti a v květnu 2019 vydal prezident Trump výkonné nařízení, kterým zakázal využívat zařízení Huawei v amerických sítích. Administrativa začala mimo jiné vyvíjet tlak na své spojence, aby rovněž zakázali působení čínské společnosti na svých trzích. Nicméně hned poté, co americký prezident označil čínskou firmu za „velmi nebezpečnou“, uvedl, že by Huawei mohla být součástí obchodní dohody.[1]

V návaznosti na Trumpův projev se v této bakalářské práci věnuji politice bývalého amerického prezidenta Donalda Trumpa vůči čínské společnosti Huawei a tomu, jakou roli sehrála kybernetická bezpečnost v rozhodnutí Trumpovy administrativy. Téma práce jsem si vybrala z několika důvodů. Hlavním důvodem je jeho aktuálnost, neboť otázka geopolitické rivality mezi Spojenými státy a Čínskou lidovou republikou zůstává neustále relevantní, což se odráží i v oblasti kybernetické bezpečnosti a technologickém závodění, jak je patrné z kauzy Huawei.

[1] Jana Lipská, „Podle Trumpa by mohla být společnost Huawei součástí obchodní dohody, firmu ale označuje za nebezpečnou.“ *Seznam Zprávy*, 24.května 2019, https://www.seznamzpravy.cz/clanek/podle-trumpa-by-mohla-byt-spolecnost-huawei-soucasti-obchodni-dohody-firmu-ale-oznacuje-za-nebezpecnou-72593. (staženo 17. dubna 2024).

Je totiž neobvyklé, aby stát otevřeně vystupoval proti soukromému podniku. USA podezřívají společnost Huawei z provádění kyberšpionáže ve prospěch Pekingu. Proti tomu se ostře ohradila čínská vláda, která tvrdí, že Washington se snaží zpomalit její úspěšný hospodářský růst prostřednictvím blokací čínských společností. Čínská společnost získala nelichotivou reputaci i v českém prostředí, když Národní úřad pro kybernetickou a informační bezpečnost vydal již v roce 2017 varování před používáním softwaru a hardwaru společnosti Huawei.[2] Z tohoto důvodu je téma relevantní také pro českou společnost.

Cílem práce je podrobně zkoumat faktory, které vedly k zákazu společnosti Huawei ve Spojených státech. Za účelem podrobného zkoumání této problematiky si v rámci této práce kladu následující otázky: Proč se rozhodla administrativa Donalda Trumpa zakázat společnost Huawei jako poskytovatele 5G služeb na americkém i celosvětovém trhu? Jaké byly klíčové faktory tohoto zákazu a jednalo se převážně o obavy z kybernetické bezpečnosti?

K zodpovězení hlavní výzkumné otázky budu využívat postupy spojené s analýzou zahraniční politiky (*Foreign policy analysis*, FPA), která ve svém základu zkoumá, jak stát vytváří svou zahraniční politiku. Tímto přístupem se zaměřím na klíčové aktéry v politice vůči Huawei a na samotnou roli prezidenta. Dále práce bude pracovat s metodou *process tracing*, která umožní identifikovat potenciální příčiny Trumpova rozhodnutí. Výzkum práce je ze své podstaty spíše kvalitativním, neboť jde o analýzu konkrétní události. Z metodologického hlediska se dá práce charakterizovat jako explanatorní případová studie. Podrobný výzkum tohoto případu tedy přispěje k lepšímu porozumění vztahů mezi Spojenými státy a Čínskou lidovou republikou.

Na základě stanoveného cíle je tato práce rozdělena do pěti kapitol. První kapitola se zabývá teoreticko-metodologickým rámcem práce a vysvětluje koncept analýzy zahraniční politiky a dále metodu *process tracing*. Druhá kapitola se věnuje společnosti Huawei, jejím vztahem k ČLR a popíše, co je technologie 5G a její vliv na kybernetickou bezpečnost. Třetí kapitola shrne kroky Trumpovy administrativy vůči společnosti Huawei. Čtvrtá část analyzuje možné důvody, proč se administrativa rozhodla zakázat společnost Huawei na americkém i světovém

[2] „Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou“, Národní úřad pro kybernetickou a informační bezpečnost,17.prosince 2018, https://nukib.gov.cz/cs/infoservis/aktuality/1303-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/ (staženo 19. listopadu 2023).

trhu. Primárně je kladen důraz na kybernetickou bezpečnost. Získané poznatky a odpovědi na výzkumnou otázku a výsledky práce jsou shrnuty v závěru práce.

Rozbor literatury

Pro zpracování této práce jsem použila kombinaci primárních a sekundárních zdrojů. Vzhledem k nedostatku domácí literatury jsem ve většině případů využila zahraniční zdroje. Mezi primární zdroje patří dokumenty Bílého domu, jako například *National Strategy to Secure 5G* od bývalého amerického prezidenta Donalda Trumpa, které mi ukázaly, jak administrativa formulovala téma kybernetické bezpečnosti a 5G technologií. Paměti Johna Boltona, bývalého poradce pro národní bezpečnost během prezidenství Trumpa, z knihy *The Room Where It Happened: A White House Memoir,* mi pomohly pochopit, jaký proces vedl k zákazu společnosti Huawei a samotný postoj bývalého prezidenta k této otázce. Za silnou stránku knížky považuji právě Boltonovo líčení schůzek s Trumpem. Jeho živý popis chaosu během těchto setkání nabízí hlubší vhled do dynamiky, konfliktů a procesů rozhodování, které se odehrávaly za zavřenými dveřmi Bílého domu. Nicméně Bolton neprozrazuje konkrétní metody zpravodajských služeb, které by podpořily rozhodnutí Trumpovy administrativy zakázat čínskou společnost na základě ochrany národní bezpečnosti. Celkově proto práce bude převážně vycházet ze sekundárních zdrojů, jako jsou knižní publikace, články z elektronických časopisů a novinové články, neboť se jedná o aktuální téma.

Analýza Adama Segala v knize *The Hacked World Order* upevňuje postavení Číny a Spojených států jako hlavních kybernetických velmocí, jelikož disponují rozsáhlou vyspělou technologickou infrastrukturou. Kybernetický prostor se stal novým polem, na kterém se odehrávají geopolitické konflikty, a proto je zahrnut v otázkách národní bezpečnosti.[3] Sbor náčelníků štábu (*Joint Chiefs of Staff*, JCS) za prezidenta Donalda Trumpa charakterizoval kyberprostor jako rozsáhlou globální doménu v informačním prostředí, která zahrnuje nejen internet, ale také telekomunikační sítě, počítačové systémy a širokou škálu zařízení. Některé státy mohou využívat kyberprostor k útokům nebo špionáži proti Spojeným státům.[4] Národní

[3] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016), 40.

[4] Joint Chiefs of Staff, *Joint Publication 3-12 (R): Cyberspace Operations* (Washington D.C., 2018), 6-8, https://irp.fas.org/doddir/dod/jp3_12r.pdf (staženo 11.prosince.2023).

kybernetická bezpečnost je definovaná Nazli Chourciovou a Davidem Clarkem v jejich knize *International Relations in the Cyber Age* jako schopnost státu chránit sebe a své instituce před hrozbami, špionáží, sabotáží, zločinem, podvody, krádežemi identit a dalšími destruktivními činnostmi v kyberprostoru.[5]

V literatuře se často diskutuje o vzestupu Číny jako globální mocnosti a jeho dopadu na hegemonii USA. John Mearsheimer považuje Čínu za přímou hrozbu pro dominanci Spojených států a předpovídá nevyhnutelný konflikt mezi zeměmi[6], zatímco Graham Allison představuje koncept Thukydidova poučení, který tvrdí, že když rostoucí mocnost ohrožuje stávající, válka je pravděpodobným výsledkem, ale není nevyhnutelná.[7] Ekonomický vzestup Čínské lidové republiky také formoval interpretaci čínských aktivit v kyberprostoru. Kybernetická špionáž, kterou Čína využívá k posílení své pozice, údajně může sloužit jako klíčový nástroj pro změnu světové mocenské rovnováhy– jak poukazuje Brandon Valeriano ve své knize *Cyber Strategy: The Evolving Character of Power and Coercion*. Tato kyberšpionáž umožní špehující straně získat informace, které pak mohou přispět k jejímu hospodářskému nebo technologickému rozvoji.[8] Jason R. Fritze ve své knize *China's Cyber Warfare* rovněž upozorňuje na to, že kyberprostor je úzce spojen s ekonomickým růstem a vojenskou expanzí Číny. Mimo jiné uvádí, že krádeží duševního vlastnictví a obchodních tajemství může Čína posílit svou hospodářskou konkurenceschopnost.[9]

Například kniha *Techno-Geopolitics: US-China Tech War and the Practice of Digital Statecraft* od Pak-nung Wonga zkoumá geopolitické soupeření mezi Spojenými státy a Čínou v rámci závodu o globální technologickou nadvládu. Wong uvádí, že obchodní válka mezi USA a Čínou je více než jen spor o cla a obchodní deficit; reflektuje hlubší rivalitu v oblasti technologického vedení. Srovnává současnou situaci s obdobím po druhé světové válce, kdy vzestup Japonska

[5] Nazli Choucri a David Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma* (Cambridge, MA: MIT Press, 2018), 95.
[6] John J. Mearsheimer, *The Tragedy of Great Power politics (*New York: W. W. Norton & Company, 2001), 4.
[7] Graham Allison, *Destiny for War – Can America and China Escape the Thucydides's Trap?* (Boston: Houghton Mifflin Harcourt, 2017)*,* 208-210.
[8] Brandon Valeriano, „ China and the Technology Gap: Chinese Strategic Behavior in Cyberspace", in *Cyber Strategy: The Evolving Character of Power and Coercion*, ed. Brandon Valeriano, Benjamin Jensen a Ryan C. Maness (Oxford: Oxford University, 2019), 158–162.
[9] Jason R. Fritz, *China's Cyber Warfare: The Evolution of Strategic Doctrine* (Lanham, MD: Lexington Books,2017), 7-12.

vyvolal podobná napětí se Spojenými státy. Technologický rozvoj Číny je viděn jako výzva pro americkou průmyslovou dominanci, což vede k různým obchodním restrikcím a strategickým krokům, jako je například světový zákaz společnosti Huawei. Technologii 5G považuje za klíčový prvek této rivality, která může být v kontextu realismu pojímána jako zdroj „strukturální moci".[10] Sin-jen Pcheng ve svém článku *The Essence and Impact of US-China Technology Competition* popisuje technologické soupeření jako zápas o přední světové postavení, neboť právě technologie jsou hnacím motorem k získání či udržení vlivu pro velmoci. Ve svém textu zdůrazňuje, že technologické pokroky nejen formují moderní svět, ale také posilují moc a vliv jednotlivých států.[11]

Velkým přínosem pro mě byla knížka *Huawei Goes Global Volume I: Made in China for the World*. Tato kniha zkoumá složitou roli společnosti Huawei v obchodním sporu mezi USA a Čínou a její vazby na čínskou vládu. Dále se zabývá rolí společnosti Huawei v rámci rozsáhlejších čínských iniciativ, jako je Hedvábná stezka (BRI). Autoři v knize analyzují, jak je technologický pokrok Huawei v oblasti 5G a umělé inteligence propojen s čínskou geopolitickou strategií. Je však důležité brát na vědomí, že kniha byla vydána v roce 2020, kdy se technologie 5G nacházela v raných stádiích vývoje a její budoucnost byla nejasná. V knize je také opomíjena role kybernetické bezpečnosti v rámci tohoto konfliktu a proč čínská společnost Huawei představuje potenciální riziko pro národní bezpečnost.

Ačkoliv zmíněná literatura poskytuje cenné poznatky o různých aspektech kauzy Huawei, čínské kyberšpionáži a technologickém soupeření mezi USA a Čínou, nezabývá se dostatečně jednáním vládních agentur a samotnou rolí bývalého prezidenta Trumpa. Rovněž chybí zkoumání kauzy Huawei z hlediska kybernetické bezpečnosti, zejména pokud jde o možnou existenci zadních vrátek v jejích produktech, která by mohla být využita čínskou vládou ke špionážním účelům.

[10] Pak Nung Wong, *Techno-Geopolitics: U.S.-China Tech War and the Practice of Digital Statecraft* (London: Routledge, 2021), 115-116,120.
[11] Xinyan Peng, „The Essence and Impact of US-China Technology Competition*", Advances in Social Science, Education and Humanities Research*, 11.července 2023, 755, https://doi.org/10.2991/978-2-38476-062-6_97 (staženo 11. dubna 2024).

1. Teoreticko-metodologická část

1.1 Analýza zahraniční politiky

Zahraniční politika je soubor opatření, jež provádí politická autorita v mezinárodním prostředí. Skládá se z řady strategií, cílů, opatření, metod a multilaterálních dohod, na jejichž základě spolu státy jednají. Na utváření zahraniční politiky má vliv řada aktérů a institucí v demokratickém systému. Mezi hlavní tvůrce zahraniční politiky se řadí vládní představitelé států, mimo jiné premiér nebo ministr zahraniční.[12]

Analýza zahraniční politiky (FPA) vznikla jako samostatný obor v rámci mezinárodních vztahů (MV). Na rozdíl od MV, jejichž cílem je interpretovat celkový mezinárodní systém, se FPA zaměřuje na faktory, které přispěly k vládnímu rozhodnutí. Analytici zahraniční politiky kladou důraz na zahraničně politický proces. Jsou přesvědčeni, že studium aktérů, jejich motivací, rozhodovacích procesů a širšího kontextu umožní předložit detailní zhodnocení zahraniční politiky.[13] Akademici se shodují vesměs v tom, že analýza zahraniční politiky uplatňuje mnoho teorií MV. Každý postup může vycházet z jiných ústředních bodů, podle kterých jsou tvořeny zájmy států. Například liberálové kladou důraz na spolupráci mezi státy. Domnívají se, že vzájemná ekonomická závislost a společné zájmy mohou vést k mírovým vztahům a spolupráci. Na druhé straně stojí realisté, kteří prosazují zahraniční politiku řízenou striktně podle národních zájmů. Stát je považován za aktéra v mezinárodních vztazích a jeho hlavním cílem je zajištění vlastní bezpečnosti.[14]

Hlavními teoretickými přístupy, které budou pro tuto práci klíčové jsou defenzivní a ofenzivní realismus. Oba přístupy se shodují v tom, že přežití je primárním motivem státu v anarchickém systému, což znamená, že neexistuje vyšší centralizovaná autorita nad státy. Nicméně pro defenzivní realisty je většina států mocnostmi, usilující o udržení statusu quo a o vyvážení moci. To povede k udržení stabilního mezinárodního systému a zajištění svého vlastního bezpečí. Defenzivní realisté dodávají, že konflikt je někdy nevyhnutelný, například pokud je stát

[12] Jean-Frédéric Morin a Jonathan Paquin, *Foreign Policy Analysis: A Toolbox (*London: Palgrave Macmillan, 2018), 23-24.
[13] Chris Alden a Amnon Aran, *Foreign Policy Analysis: New Approaches* (London: Routledge, 2017), 7-8.
[14] Georg Sørensen, Jørgen Møller a Robert H. Jackson, *Introduction to International Relations: Theories and Approaches* (Oxford: Oxford University Press, 2022), 251-252.

napaden jiným státem a jeho bezpečnost je ohrožena. Na druhou stranu ofenzivní realisté tvrdí, že státy se spíše snaží maximalizovat svou moc než zajišťovat bezpečnost. Podle ofenzivního realismu státy nespoléhají pouze na udržení rovnováhy sil, jelikož věří, že to samo o sobě není dostatečné k zajištění bezpečnosti. Podle Mearsheimera anarchický mezinárodní systém a nejistota ohledně současných a budoucích záměrů jiných států, jako je Čína, nutí Spojené státy maximalizovat svou mocenskou pozici. Zdůrazňuje, že konečným cílem každého státu je stát se hegemonem v systému.[15]

Kromě obecných teoriích v rámci studia mezinárodních vztahů existují další přístupy, které můžeme aplikovat pro analýzu zahraniční politiky. Graham Allison ve svém díle *Essence of Decision: Explaining the Cuban Missile Crisis* představil tři koncepční modely, které umožní pochopit fungování rozhodovacích procesů americké vlády během Karibské krize. Jedná se o model racionálního činitele, organizační model a byrokratický model. Nejčastěji citovaným přístupem k analýze zahraniční politiky je model racionálního činitele (*rational actor model*).[16] V tomto modelu se předpokládá určitá účelnost rozhodovaní, tedy, že si vláda z možností, jež se jí nabízejí, zvolí tu, která nejpravděpodobněji povede k dosažení stanoveného cíle. Racionální aktér se v tomto modelu rozhoduje na základě logického hodnocení informací a snaží se optimalizovat výsledky ve prospěch národního zájmu.[17] V případě kauzy Huawei došla americká vláda k závěru, že priorita ochrany národní bezpečnosti má přednost před ekonomickými zájmy.

Svůj původní model Allison posouvá na organizační model, kdy stát není již chápán jako unitární aktér, ale spíše jako konglomerát volnějších organizací, které často nepracují společně při řešení problémů. Zahraniční politika je tudíž v tomto případě viděna jako výsledek organizačního procesu. Každá organizace se zaměřuje na odlišný aspekt problému v souladu se svojí specializací. Tímto způsobem každá instituce přispívá svým dílem k řešení strategické výzvy. Naproti tomu byrokratický model předpokládá, že rozhodnutí je výsledkem

[15] Steven E. Lobell, *Structural Realism/Offensive and Defensive Realism.* Oxford Research Encyclopedia of International Studies*,* 22.prosince 2017, https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-304 (přístup 27.listopadu 2023).
[16] Alden a Aran, *Foreign Policy Analysis: New Approaches*, 57.
[17] Sørensen, Møller, a Jackson, *Introduction to International Relations: Theories and Approaches*, 254.

vyjednávání, kompromisů a politického soupeření, nikoli výsledkem racionálního procesu založeného na objektivní analýze a systematickém vyhodnocování možností. Zákaz Huawei by byl tedy ovlivňován různými vládními úřady, bezpečnostními agenturami nebo byrokratickými strukturami.[18]

Kritici modelu upozorňují na to, že model může podceňovat roli prezidenta ve státním rozhodovacím procesu.[19] V americkém politickém systému má prezident značnou moc nad tím, kdo bude zastávat klíčové pozice ve vládě, ale i nad samotným procesem rozhodování. I přesto, že prezident nemůže sám vydávat zákony, disponuje nástroji, které mu umožňují formovat zahraniční politiku. Prezident má k dispozici několik metod, jak toho dosáhnout. Například vydávání výkonných nařízení, memorand a nařízení týkajících se národní bezpečnosti.[20] Podle Roberta Jervise s každým novým vůdcem, který se ujme moci, máme šanci empiricky zkoumat, jaký vliv má osobnost lídra na směřování zahraniční politiky. Prezidentství Donalda Trumpa poskytlo unikátní příležitost pro zkoumání teorie, podle které politický styl a vůdcovský styl (*leadership style*) mohou výrazně ovlivnit zahraniční politiku, neboť jeho přístup se odlišoval od jeho předchůdců.[21] Při formování Trumpova přístupu k zahraniční politice sehrály klíčovou roli jeho osobní přesvědčení, politický styl a rétorika. Jeho prezidentství bylo charakterizováno nekonvenčním diplomatickým přístupem a rozsáhlým využíváním sociálních médií.

Podle Toma Lourieho byl rozhodovací proces Donalda Trumpa charakterizován intuitivním přístupem.[22] Thomas Preston, expert na analýzu stylu vedení (*leadership trait analysis*), uvádí, že bývalý americký prezident neměl silnou vazbu ke skupinám. Ti, kteří mu lichotili byli součástí jeho kruhu, ale mohli být snadno odvrženi, když se dostali do jeho nepřízně. Během prezidentské kampaně slíbil Trump prosazovat agendu „America First", která klade důraz na národní zájmy před globální spoluprací. Podle Prestona však Trump spíše využíval téma

[18] Morin a Paquin, *Foreign Policy Analysis: A Toolbox,* 295,307.
[19] Sørensen, Møller a Jackson, *Introduction to International Relations: Theories and Approaches*, 255.
[20] Sabrina Pastorková, „Foreign Policy of Trump's Administration: Withdrawal from the Paris Accord through the Lens of Two-Level Game Theory" (diplomová práce, Univerzita Karlova, 2019), vedoucí práce doc. PhDr. Jan Karlas, M.A., Ph.D., 12.
[21] Robert Jervis, „President Trump and International relations theory ", in *Chaos in the Liberal Order: The Trump Presidency and International Politics in the Twenty-First Century*, ed. Robert Jervis, Francis J. Gavin, Joshua Rovner a Diana N. Labrosse (New York: Bloomsbury Publishing, 2013), 24.
[22] Tom Lourie, , "The Decision Calculus of Donald Trump", in *How Do Leaders Make Decisions?*, ed. Alex Mintz A Dmitry Adamsky (Leeds: Emerald Publishing Limited, 2019), 33.

nacionalismu k přilákání stoupenců, než aby byl jeho silným zastáncem.[23] Obecně se má za to, že Trumpův přístup k zahraniční politice byl transakční. Tento postoj spočívá v řešení politických otázek stejným způsobem, jako by to byly obchodní transakce. Transakční přístup k zahraniční politice se zaměřuje na dosažení okamžitých výsledků. Dohody, které vyžadují delší časové období, aby přinesly výnosy, do transakčního modelu nezapadají. Trump se domníval, že jeho schopnosti a zkušenosti v obchodování spolu s ekonomickou a strategickou silou USA mu umožní vyjednávat bilaterální dohody, které si dle něj jeho předchůdci, zejména Obama, nedokázali zajistit.[24]

1.2 Process tracing

Americký politolog Collier definuje *process tracing* jako systematické zkoumání vybraných důkazů za účelem porozumění jednotlivým krokům nebo procesům, které jsou analyzovány v kontextu předem stanovených výzkumných otázek a hypotéz.[25] Hlavním cílem *process tracing* je testovat, budovat nebo vysvětlit kauzální mechanismy, neboli faktory, které ovlivnily průběh událostí a nakonec vedly k danému výsledku.[26] Podle sociologa Mazáka je úkolem výzkumníka ověřit, zda předpokládaný kauzální mechanismus vysvětluje zkoumaný případ. Pro tento účel můžeme začít hledáním potenciálních důkazů, které naznačují, že tento mechanismus skutečně ovlivňuje zkoumanou situaci.[27] Beach a Pedersen navrhují, že k identifikaci těchto konkrétních stop lze využít kreativní brainstorming, ale také se dá inspirovat existující literaturou.[28]

[23] Martha Cottam, „Foreign Policy Decision Making in the Trump Administration," in *The Trump Doctrine and the Emerging International System*, ed. Stanley A. Renshon, Peter Suedfeld (London: Palgrave Macmillan, 2021), 133-138.
[24] C. J. Bowling, Fisk, J. M., A. Morris, J, „Seeking Patterns in Chaos: Transactional Federalism in the Trump Administration's Response to the COVID-19 Pandemic ", *The American Review of Public Administration*, 50(6-7), 512-518, (16.června 2020), https://doi.org/10.1177/0275074020941686 (staženo 4.dubna 2024)
[25] Nicholas R. Smith, „Using Process-Tracing to Drive Foreign Policy Analysis: Strengths and Weaknesses in the Context of Analyzing the Foreign Policies of the EU and Russia in the Context of the Ukraine Crisis." In *Sage Research Methods Cases Part 2*. London: Sage Publications Ltd., 2024. https://doi.org/10.4135/9781526462404.
[26] Derek Beach a Rasmus Brun Pedersen, *Process-Tracing Methods: Foundations and Guidelines* (Ann Arbor : University of Michigan Press, 2019),11-12.
[27]Jaromír Mazák, Občanská *společnost jako aktér politického procesu*. Disertační práce, vedoucí Císař, Ondřej. Praha: Univerzita Karlova, Filozofická fakulta,2019, 104.
[28] Derek Beach a Rasmus Brun Pedersen, *Process-Tracing Methods: Foundations and Guidelines,* 87-88.

Akademici rozlišují tři hlavní způsoby využití *process tracing*: konstrukce teorie, testování teorie a vysvětlování výsledků (*explaining outcome*).[29] Pro moji práci jsem si zvolila *explaining outcome* metodu, která se často používá ve výzkumech zaměřených na analýzu historických událostí. Cílem této metody je vysvětlit charakter konkrétních událostí, a tudíž není plně zakořeněna v teorii. Když používáme PT máme známou závislou proměnnou Y (v našem případě je to Trumpovo výkonné nařízení vůči Huawei), ale neznáme nezávislou proměnnou X, což je v tomto případě příčina, která vedla k tomuto kroku, a proto se jí snažíme vysvětlit. Při použití *explaining-outcome process tracing* je klíčové pochopit kauzální mechanismus podrobněji než u jiných metod sledování procesu, jak uvádějí autoři Beach a Pedersen.[30] To je způsobeno tím, že při vysvětlování příčiny historické události se zohledňují i její jedinečné a specifické součásti, které jsou pro danou událost charakteristické a nelze je nalézt jinde. Právě proto má tato metoda dobré uplatnění ve FPA. Analýza zahraniční politiky pomocí PT je vhodná pro přístupy, které se snaží porozumět motivacím, přesvědčením a jednáním jednotlivých aktérů v rámci procesu zahraniční politiky.[31]

[29] Ibid, 13.
[30] Ibid, 281–283.
[31] Peter A. Mello a Frank Ostermann, eds. *Routledge Handbook of Foreign Policy Analysis Methods*, (London: Routledge,2022), https://doi.org/10.4324/9781003139850, 405.

2. Společnost Huawei, Čína, 5G a kybernetická bezpečnost

2.1 Čínská vláda a Huawei

Huawei, čínská soukromá společnost, je největší společností vyrábějící telekomunikační zařízení 5G. Byla založena v roce 1987 bývalým inženýrem Čínské lidové armády Žen Čeng-fejem právě v té době, kdy byla Čínská lidová republika stále silně závislá na dovozu telekomunikačních zařízení. Vznik Huawei souvisí s obdobím klíčových ekonomických reforem pod vedením Teng Siao-pchinga. Tyto reformy podpořily rozvoj technologického sektoru v Číně.[32] Původně se Huawei zabývala dovozem telekomunikačních přepínačů pro čínskou armádu, avšak brzy začala vyvíjet své vlastní technologie a postupem času se Huawei stala jedním z nejvýznamnějších světových výrobců telekomunikačních zařízení.[33]

Společnost se na svých internetových stránkách chlubí tím, že je vlastněna svými zaměstnanci. Žádný jednotlivec nemůže vlastnit akcie ve společnosti Huawei, aniž by byl jejím zaměstnancem. K roku 2018 bylo zaznamenáno, že akcie společnosti Huawei vlastnilo více než 96 tisíc jejích zaměstnanců. Dokonce i zakladatel firmy drží pouze malý podíl, který činí 1,14 %. Huawei rovněž odmítá tvrzení o tom, že by byla vlastněna, kontrolována nebo jakkoliv jinak spojena s vládou.[34] Nicméně někteří analytici se domnívají, že úspěch společnosti Huawei je podmíněn čínskou vládní podporou, avšak rozsah, do jaké tato podpora přispěla k růstu Huawei, je stále předmětem diskusí.[35]

Například ve studii z roku 2005 od kalifornské výzkumné instituce *RAND Corporation*, která zkoumala vývoj čínského obranného a průmyslového komplexu, byla společnost Huawei (spolu s dalšími čínskými IT firmami) označena za součástí tzv. techno-nacionalistické strategie. Tato strategie spočívá v úzké spolupráci mezi soukromými čínskými firmami, státními výzkumnými institucemi a armádou. Soukromé společnosti, jako je Huawei, hrají v této strategii klíčovou

[32] Jean-Marc F. Blanchard, „Helping Hands for Huawei: Dialing into China's Technology Policy to Understand Its Contemporary Support for Huawei" in *Huawei Goes Global: Volume I: Made in China for the World,* ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann, (London: Palgrave Macmillan, 2020), 68-70.
[33] Francis Schortgen, „Weaponizing Globalization: Chinese High-Tech in the Crosshairs of Geopolitics" in *Huawei Goes Global: Volume I: Made in China for the World,* 51-53.
[34] „ Who owns Huawei?'', *Huawei*, https://www.huawei.com/ke/facts/question-answer/who-owns-huawei (staženo 7.prosince 2023).
[35] Jill C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests(Washigton D.C:* Congressional Research Service, 5.ledna 2022), 38, https://crsreports.congress.gov/product/pdf/R/R47012/2 (staženo 2. prosince 2023).

roli. Jsou financovány státem, získávají podporu od armády a státních bank a zaměřují se na dosažení komerčního úspěchu jak na domácím, tak na mezinárodním trhu. Mimořádně úzké vazby mezi Huawei a PLA znamenají, že Čínská lidová osvobozenecká armáda může mít přímý přístup k technologické infrastruktuře společnosti Huawei.[36]

Jak ukázal americký deník *Wall Street Journal,* čínská státní podpora pro společnost Huawei dosáhla v roce 2018 výše až 75 miliard dolarů. Největší část této podpory, přibližně 46 miliard dolarů, pocházela z půjček, úvěrových linek a dalších forem finanční podpory poskytovaných státními věřiteli. Společnost Huawei ve svých prohlášení uvádí, že obdržela jen malou podporu od čínské vlády na svůj výzkum, včetně daňových úlev pro technologický sektor. Podle společnosti se nejednalo o nic neobvyklého a stejné podmínky byly dostupné i pro ostatní subjekty na čínském trhu.[37] Nicméně další vládní financování společnosti Huawei můžeme vidět například v Africe. Podle Cobuse van Stadena, výzkumného pracovníka v Johannesburgu, vybudovala čínská společnost přibližně 70 % sítí 4G na africkém kontinentě, čímž výrazně předstihla své evropské konkurenty, jako jsou například Nokia nebo Ericsson.[38] June Senová z Čínsko-afrického výzkumného institutu z Univerzity Johnse Hopkinse, uvádí, že vládní podpora umožňuje Huawei poskytovat výhodnější ceny než třeba jiní konkurenti na trhu.[39]

Huawei je příkladem rostoucích přímých zahraničních investic z Číny do rozvojových zemí, symbolizujícím čínské globální ambice. Klíčovou součástí této expanze je iniciativa Nová hedvábná stezka (BRI), ambiciózní projekt zaměřený na posílení infrastruktury a obchodních vazeb Číny s různými světovými regiony, včetně rozvojových zemí. Všechny africké země, které se připojily k čínské iniciativě BRI, s výjimkou Čadu, povolily společnosti Huawei účast na svých sítích 5G.[40] Je nutné ale poukázat na zprávu francouzského deníku *Le Monde* z roku 2018, podle níž počítačový systém v sídle Africké unie v Addis Abebě, který z velké části

---

[36] Evan S. Medeiros, Roger Cliff, Keith Crane a James C. Mulvenon. *A New Direction for China's Defense Industry*. 1st ed. RAND Corporation, 2005, http://www.jstor.org/stable/10.7249/mg334af, 206-207.
[37] Chuin-Wei Yap , „State Support Helped Fuel Huawei's Global Rise" , *The Wall Street Journal,* 25.prosince 2019, https://www.wsj.com/articles/state-sup- port-helped-fuel-huaweis-global-rise-11577280736 (staženo 27.listopadu 2023).
[38] Amy Mackinnon, „For Africa, Chinese-Built Internet Is Better than No internet at All, " *Foreign Policy,*19. května 2019. https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/(staženo 27.listopadu 2023).
[39]Jordan Link, „How Huawei Could Survive Trump", *Washington Post*. 10.června 2019. https://www.washingtonpost.com/politics/2019/06/10/what-do-we-know-about-huaweis-africa-presence/, (staženo 27.listopadu 2023).
[40] Shirley Ze Yu , „All Under Huawei: China's New Vision for a Tech Sinica" in *Huawei Goes Global: Volume I: Made in China for the World,* 91-92.

instalovala společnost Huawei, sloužil ke špionážním aktivitám. Během pěti let docházelo k přenášení dat na servery v Šanghaji, což naznačuje možné nekalé praktiky společnosti Huawei, které pak mohly vést ke shromažďování informací o národní bezpečnosti ve prospěch Pekingu.[41]

2.2 5G síť a kybernetická bezpečnost

Bezdrátová technologie páté generace neboli 5G, představuje klíčovou telekomunikační infrastrukturu, která je určena k podpoře a rozvoji chytrých měst, autonomních vozidel, pokročilých aplikací umělé inteligence a řady dalších inovativních technologických řešení. Jádrem 5G je vysokorychlostní, stabilní bezdrátové připojení, které umožní rychlejší přenos dat a sníží dobu odezvy (latenci), což je kriticky důležité pro aplikace vyžadující rychlou reakci v reálném čase.[42] Například právě ve zdravotnictví umožní 5G rychlejší a spolehlivější dálkové monitorování pacientů. Ačkoli 5G síť ještě nevyvolala takové nadšení jako umělá inteligence, především kvůli svému stále neúplnému pokrytí, očekává se, že do roku 2028 bude plně implementována a stane se klíčovým prvkem průmyslové revoluce 4.0.[43] S nasazením 5G sítí se očekává ekonomický boom, jak odhaduje Světové ekonomické fórum. Tato technologická revoluce však přináší také nové výzvy v oblasti kybernetické bezpečnosti, vzhledem k narůstajícímu počtu připojených zařízení a uživatelů.[44]

Z analýzy kybernetické bezpečnosti 5G sítí, kterou provedla Evropská komise v roce 2019, vyplývá, že i když byla kybernetická rizika již přítomna v předchozí generaci 4G, očekává se, že se s příchodem technologie 5G zvýší. Ve srovnání s 4G sítěmi, kde se data centralizovaně zpracovávají a ukládají, 5G sítě se přesouvají do vzdálených cloudových serverů. Tento posun k softwarově řízeným sítím v sobě skrývá potenciální bezpečnostní rizika. Například, pokud dodavatelé sítě nedodržují adekvátní postupy při vývoji softwaru, může dojít k úmyslnému

[41] Ghalia Kadiri a Joan Tilouine, „A Addis-Abeba, Le Siège de l'Union Africaine espionné par Pékin", *Le Monde*, 26. ledna 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-unionafricaine-espionne-par-les-chinois_5247521_3212.html. (staženo 17.dubna 2024)
[42] Laura Kirste a Dirk Holtbrügge, „Huawei at Bay? A View on Dependency Theory in the Information Age" in *Huawei Goes Global: Volume I: Made in China for the World,* 291.
[43] „5G et empreinte environnementale des réseaux :de nouveaux travaux de l'Arcep pour éclairer le débat et identifier des leviers d'action'', *ARCEP*, https://www.arcep.fr/actualites/actualites-et-communiques/detail/n/environnement-140122.html (staženo 7.prosince 2023).
[44] Word Economic Forum, *The Impact of 5G: Creating New Value across Industries and Society*, (Geneva: World Economic Forum, leden 2020), http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf. (staženo 7.prosince 2023).

vložení tzv. zadních vrátek do produktů, které pak umožní neoprávněný přístup nebo sledování od nežádoucích uživatelů.[45]

Je nezbytné, aby dodavatelské řetězce 5G byly spolehlivé, obzvlášť když jsou nasazeny v kritické infrastruktuře, kde by jejich selhání mohlo mít výrazný dopad na národní bezpečnost, základní potřeby obyvatelstva, zdraví lidí nebo hospodářství země.[46] Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vydal spolu s dalšími vládními orgány soubor doporučení, podle nichž je třeba posuzovat důvěryhodnost dodavatelů pro 5G sítě v České republice. Podle doporučení by dodavatel měl mít sídlo ve státě, které má demokraticky zvolenou vládu. Daná firma není nepatřičně ovlivňována zahraniční vládou a zahraničním orgánem státní správy a dále nepoužívá od domovského státu, nepřiměřených výhod.[47] Jak si můžeme všimnout, doporučení jasně neplatí pro čínskou společnost Huawei z několika důvodů. Čína není demokratický stát s plně transparentním právním systémem. Dále společnost obdržela značně větší finanční podporu od své vlády ve srovnání s podporou poskytnutou finskou vládou Nokii. Konkrétně se uvádí, že míra státní podpory, kterou Huawei získává, je až sedmnácti násobně vyšší než ta, kterou dostává Nokia od finské vlády.[48]

Úspěch Huawei v 5G sektoru není pouhá náhoda. Během let 2008 až 2018 Huawei průměrně každoročně věnovala 12,6 % ze svých tržeb na výzkum a vývoj s průměrným ročním růstem 25,6 %. V roce 2015 došlo k výraznému zvýšení investic Huawei do výzkumu a vývoje, což lze spojit s iniciativou „Made in China 2025“[49] Tato strategie, kterou představil čínský premiér Li Kche-čchiang v květnu téhož roku, měla ambici přesunout Čínu z pouhé světové továrny

[45] NIS Cooperation Group, „EU coordinated risk assessment of the cybersecurity of 5G networks“, 9. října 2019, https://www.politico.eu/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf (staženo 7.prosince 2023).

[46] „Ochrana kritické infrastruktury‘‘, Ministerstvo vnitra České republiky, https://www.mvcr.cz/chh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx (staženo 7.prosince 2023).

[47] „Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice‘‘, Národní úřad pro kybernetickou a informační bezpečnost https://www.nukib.cz/cs/infoservis/doporuceni/1801-doporuceni-pro-hodnoceni-duveryhodnosti-dodavatelu-technologii-do-5g-siti-v-ceske-republice/(staženo 7.prosince 2023).

[48] Anders Kjellman, Xiaohua Yang, Xiaobo Wu a Sun-Young Park, „Huawei’s Expansion and Nokia’s Retreat: What Lessons Can We Learn?“ in *Huawei Goes Global: Volume I: Made in China for the World,* 196.

[49] Fancis Schortgen, „Weaponizing Globalization: Chinese High-Tech in the Crosshairs“, 54. of Geopolitics“ in *Huawei Goes Global: Volume I: Made in China for the World,* 55-56.

levného zboží směrem k inovacím a službám s vyšší přidanou hodnotou. [50] Ve snaze umožnit klíčovým podnikům zaujmout vedoucí roli ve světě se program zaměřuje na deset hlavních oblastí. Například nové informační technologie, robotika, letectví, farmacie atd. patří do této iniciativy. [51] V rozhovoru pro noviny *Nikkei Asian*, jeden z rotujících předsedů společnosti Huawei, Chu Chou, uvedl, že jejich současné aktivity nemají s tímto programem příliš mnoho společného.[52] I když program „Made in China 2025“ není přímo zaměřen na odvětví telekomunikačních technologií, existují spojitosti mezi ním a Huawei. Nové informační technologie, které jsou součástí deseti klíčových odvětví v rámci nové čínské iniciativy mohou být spojeny s telekomunikačními technologiemi, jako je síť 5G.

3. Trumpova politika vůči společnosti Huawei

3.1 Huawei před Trumpovou administrativou

Řada publikací tvrdí, že problémy se společností Huawei ve Spojených státech začaly již v roce 2003,[53] kdy americká firma Cisco Systems obvinila čínská společnost z krádeže firemních tajemství a pirátství jejího softwaru.[54] Později v roce 2008 se Výbor pro zahraniční investice ve Spojených státech (*Committee on Foreign Investment in the United States*, CFIUS), chránící klíčová odvětví před zahraničním vlivem, rozhodl pozastavit plán společnosti Huawei na koupi americké společnosti 3Com.[55] Bylo tomu tak údajně proto, že společnost dodávala americké armádě anti hackerský software a čínská akvizice by představovala hrozbu pro americkou kybernetickou bezpečnost. Podobná situace se opakovala v roce 2010, kdy CFIUS vyzval

[50] Lee Branstetter a Li Guangwe, „The Actual Effect of China's 'Made in China 2025' Initiative May Have Been Overestimated" , *CEPR,* 11. srpna 2023. https://cepr.org/voxeu/columns/actual-effect-chinas-made-china-2025-initiative-may-have-been-overestimated. (staženo 19.listopadu 2023).
[51] „Made in China 2025“ , Čínská lidová republika, Státní rada (PRC State Council), 19. května 2015. http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.html. (staženo 7.prosince 2023).
[52] Li Tao, „Huawei Executive Says Company Has Little to Do with Beijing's 2025 Plan." *South China Morning Post*, 8. listopadu 2018, https://www.scmp.com/tech/enterprises/article/2172158/huaweis-ken-hu-says-company-has-little-do- beijings-ambitious-2025 (staženo 7.prosince 2023)
[53] Jean-Marc F. Blanchard, „Helping Hands for Huawei: Dialing into China's Technology Policy to Understand Its Contemporary Support for Huawei“ in *Huawei Goes Global: Volume I: Made in China for the World*, 75.
[54] Jason R. Fritz, *China's Cyber Warfare: The Evolution of Strategic Doctrine* , 7-12.
[55] Jean-Marc F. Blanchard, „Helping Hands for Huawei: Dialing into China's Technology Policy to Understand Its Contemporary Support for Huawei“ in *Huawei Goes Global: Volume I: Made in China for the World*, 75.

tehdejšího prezidenta Baracka Obamu, aby vetoval plánovanou akvizici zkrachovalé společnosti 3Leaf, která se specializovala na serverové technologie pro americkou armádu.[56]

V reakci na doporučení CFIUS a negativní ohlasy v americkém tisku napsal předseda společnosti Huawei Ken Hu otevřený dopis, v němž se snažil vyvrátit obvinění vznesená proti společnosti a vyzval americkou vládu k vyšetření této záležitosti.[57] Kongres tento apel vyslyšel a zahájil svá vlastní vyšetřování. Na základě těchto zjištění Výbor pro zpravodajské služby Sněmovny reprezentantů USA vydal varovaní, podle kterého by americké telekomunikační společnosti neměly obchodovat se společností Huawei. Jako důvod ve zprávě uvádí: „Huawei odmítl poskytnout podrobnosti o svých obchodních vztazích s čínskou armádou či zpravodajskými službami a nezveřejnil podrobnosti o rozhodovacích procesech ve firmě.“[58] Kongres dále ve své zprávě upozornil na hlavní důvod jeho znepokojení. Tím byla skutečnost, že čínské společnosti se stávají hlavními hráči v celosvětovém telekomunikačním průmyslu, oblasti, která se neodmyslitelně dotýká záležitostí národní bezpečnosti.[59] Kongres mimo jiné začal od roku 2013 přijímat zákony, které měly omezit přístup společností jako Huawei a dalších čínských telekomunikačních firem na americký trh.[60]

Společnost Huawei nakonec došla k závěru, že snaha získat americké komunikační technologie prostřednictvím akvizic představuje slepou uličku, neboť se jí opakovaně nepodařilo převzít americké podniky. Čínská firma přešla proto do ústraní a získávala technologie zřizováním společných výzkumných a vývojových center v zahraničí. Méně „čínské agresivity“ vedlo Spojené státy k tomu, že vůči společnosti Huawei polevily v ostražitosti.[61] Huawei, ačkoliv se jí nepodařilo uzavřít smlouvy s velkými americkými telekomunikačními firmami, dosáhla

---

[56] Ibid.

[57] Kathrin Hille „Huawei’s Emergence from Shadows Backfires.” *Financial Times*, 8.října 2012. https://www.ft.com/content/50ad88c2-112b-11e2-a637-00144feabdc0 (staženo 19.dubna 2024)

[58] Charles Arthur, „China’s Huawei and ZTE Pose National Security Threat, Says US Committee“, *The Guardian,* 8.října 2012, https://www.theguardian.com/technology/2012/oct/08/china-huawei-zte-security-threat (staženo 19.listopadu 2023)

[59] Michael S. Schmidt, Keith Bradshera Christine Hauser. “U.S. Panel cites risks in Chinese equipment.” *The New York Times*, 8.října 2012. https://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html.

[60] Jill C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests(Washigton D.C:* Congressional Research Service, 5.ledna 2022), 38, https://crsreports.congress.gov/product/pdf/R/R47012/2 (staženo 2. prosince 2023).

[61] Liying Wang, „China’s Huawei in the US-China Trade War in the Communications Sector Game.” In Proceedings of the 2022 2nd International Conference on Enterprise Management and Economic Development (ICEMED 2022), 485-497. Atlantis Press, 2022. doi:10.2991/aebmr.k.220603.078.

značného úspěchu na americkém trhu s menšími operátory, specializující se zejména na venkovské oblasti. Nabídkou svých produktů a služeb za konkurenčně nízké ceny lákala právě menší americké operátory, kteří pak mohli díky čínské společnosti nahradit své staromódní pevné linky vysokorychlostním internetovým připojením pro americké venkovské obyvatelstvo.[62]

3.2 Kroky Trumpovy administrativy vůči Huawei

Během prezidentského období Donalda Trumpa vztahy mezi Spojenými státy a Čínou rychle eskalovaly, což se projevilo také ve vztahu ke společnosti Huawei. Během Obamovy administrativy se USA převážně spoléhaly na intervence CFIUS, aby zabránily pokusům Huawei získat americké telekomunikační podniky nebo prodávat telekomunikační zařízení ve Spojených státech. Nicméně od nástupu Trumpa se postoj americké vlády vůči Huawei výrazně změnil. Klíčová vládní ministerstva, jmenovitě, Ministerstvo obrany, Ministerstvo obchodu, zpravodajské služby a Ministerstvo spravedlnosti, iniciovala kolektivní bojkot vůči společnosti Huawei a jejím výrobkům.

V roce 2018 vydali vedoucí zpravodajských služeb Spojených států překvapivé doporučení, aby Američané přestali kupovat výrobky Huawei. Ředitel FBI Chris Wray zdůraznil, že vpuštění společností s vazbami na zahraniční vlády do kritické infrastruktury představuje významnou hrozbu. Wray poukázal na to, že společnost Huawei, která je světovým lídrem v oblasti síťových zařízení, by zároveň mohla provádět nepozorovanou špionáž a potenciálně upravovat nebo krást informace.[63] Americké ministerstvo obrany následně zakázalo prodej výrobku Huawei na vojenských základnách v souladu se schváleným federálním Zákonem o národní obraně 2018 (*National Defense Authorization Act,* NDAA).[64] Důvodem tohoto kroku bylo potenciální nepřijatelné riziko pro personál, informace a plnění úkolů ministerstva spojené s užíváním těchto produktů. Tento zákaz byl dále posílen prostřednictvím dalšího schváleného Zákona o národní obraně za rok 2019, který obsahoval dodatečná opatření zakazující dalším

[62] William Yuen Yee, „With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?: New Perspectives on Asia" , *CSIS*, 10.prosince 2020, https://www.csis.org/blogs/new-perspectives-asia/us-restrictions-huawei-and-zte-where-will-rural-america-turn (staženo 19.listopadu 2023).

[63] Sara Salinas, „Six Top US Intelligence Chiefs Caution against Buying Huawei Phones", *CNBC*, 15.února 2018. https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html. (staženo 19.listopadu 2023).

[64] Catherine Shu, „New Defense Bill Bans the U.S. Government from Using Huawei and ZTE Tech." *TechCrunch*, 15.srpna 2018. https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-using-huawei-and-zte-tech/

vládním agenturám obchodovat s čínskými dodavateli jako Huawei.[65] V reakci na rostoucí nepřátelství USA podala společnost Huawei na americkou vládu žalobu za nespravedlivý zákaz, v níž se uvádí: „Tento zákaz je nejen nezákonný, ale také omezuje společnost Huawei v zapojení do spravedlivé hospodářské soutěže, což v konečném důsledku poškozuje americké spotřebitele"[66]

Na žádost USA o extradici byla v prosinci 2018 v Kanadě zatčena finanční ředitelka, viceprezidentka společnosti a dcera zakladatele Huawei Meng Wan-čou za údajné porušení amerických sankcí vůči Íránu. Trump otevřeně naznačil, že pokud by s ním byl Peking ochoten uzavřít obchodní dohodu, mohl by zasáhnout do probíhajícího trestního řízení.[67] Kanadský ministr zahraničních věcí okamžitě zdůraznil, že soudní řízení by nemělo sloužit politickým účelům.[68] Později Ministerstvo spravedlnosti USA obvinilo Huawei a Meng z vydírání za účelem krádeže obchodních tajemství, technologií a duševního vlastnictví amerických společností. V obžalobě dále vyšlo najevo, že interní politikou společnosti Huawei bylo podporovat a odměňovat zaměstnance za krádež duševního vlastnictví konkurentům nebo dodavatelům. Jinými slovy, všichni zaměstnanci společnosti Huawei byli povzbuzováni k provádění průmyslové špionáže po celém světě.[69]

Podle Johna Boltona, bývalého poradce pro národní bezpečnost Donalda Trumpa, začala Trumpova administrativa v roce 2019 během obchodních jednání s Čínou připravovat návrhy výkonných nařízení, které měly zajistit ochranu telekomunikačních sítí. Jejich provedení nebylo snadné, jelikož se část administrativy bála důsledku zákazu společnosti Huawei na obchodní jednání s Čínou. Někteří představitelé z administrativy si také mysleli, že Huawei nepředstavuje hrozbu. Firmu považovali jen za dalšího konkurenta. Podle nich se „ochranitelé" národní

---

[65] Jill C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests(Washigton D.C:* Congressional Research Service, 5.ledna 2022), 14. https://crsreports.congress.gov/product/pdf/R/R47012/2 (staženo 2. prosince 2023).

[66] Lily Kuo, „Huawei Sues Us over Government Ban on Its Products." *The Guardian*, 7.března 2019. https://www.theguardian.com/world/2019/mar/07/huawei-sues-us-over-government-ban-on-its-products. (staženo 19.listopadu 2023).

[67] Andy Blatchford a Leah Nylen, „Trump's Comments about Huawei Exec's Arrest to Take Center Stage in Extradition Fight." *POLITICO*, 15.června 2020, https://www.politico.com/news/2020/06/15/trump-china-trade-deal-huawei-executive-extradition-319642. (staženo 19.listopadu 2023).

[68] Huileng Tan, „Trump Faces Pushback after Saying He May Intervene in Arrest of Huawei Executive." *CNBC*, 13. prosince 2018. https://www.cnbc.com/2018/12/13/huawei-cfo-arrest-pushback-against-trump-who-says-he-may-intervene.html. (staženo 19.listopadu 2023).

[69] Daniel Gonzalez, Julia Brackup, Spencer Pfeifer a Timothy M. Bonds, „Securing 5G: A Way Forward in the U.S. and China Security Competition. " Santa Monica, CA: *RAND Corporation*, 2022, 37. https://www.rand.org/pubs/research_reports/RRA435-4.html.

bezpečnosti, jako byl Bolton, snažili prostřednictvím nového opatření pomoc americkým firmám a poškodit Huawei.[70] Nakonec ale Trump v květnu vydal výkonné nařízení, které zakazuje americkým firmám využívat technologie či služby od jakékoli entity, která představuje hrozbu pro americkou národní bezpečnost.[71] Nařízení sice nejmenuje žádnou konkrétní společnost, ale obecně se má za to, že tento krok byl namířen proti společnosti Huawei.[72] Téhož dne americké Ministerstvo obchodu zařadilo čínskou společnost na „seznam subjektů", což je černá listina společností, které vyžadují souhlas od americké vlády, aby mohly nakupovat součástky od amerických společností.[73]

V červnu 2019, během summitu G20 v Ósace, došlo mezi Spojenými státy a Čínou k důležitému diplomatickému kroku. Obě země se dohodly na dočasném přerušení eskalace obchodní války, což bylo klíčové pro zklidnění napjatých vztahů a obě strany tak otevřely možnost dalšího jednání. Například, v rámci těchto jednání, Trump dále uvedl, že umožní americkým společnostem prodávat své výrobky čínskému podniku a naznačil, že by ji v budoucích obchodních rozhovorech s ČLR možná odstranil ze seznamu.[74] Jakmile Trumpova administrativa začala zmírňovat omezení, předložil Kongres návrh zákona, který ukládal restrikce vůči čínské technologické firmě Huawei. Odstranění Huawei ze seznamu subjektů by vyžadovalo souhlas Kongresu. Dále se Sněmovna reprezentantů rozhodla zakázat americké vládě využívat federální finanční prostředky na nákup telekomunikačního vybavení a služeb od společnosti Huawei.[75]

V průběhu pandemie COVID-19 se americko-čínské vztahy zhoršovaly, přičemž prezident Trump obvinil Čínu z nedostatečné reakce na šíření koronaviru a naznačil, že Spojené státy by

---

[70] John Bolton, *The Room Where It Happened (New* York City: Simon & Schuster LLC, 2020), 201.

[71] Donald J. Trump, „ Executive Order on Securing the Information and Communications Technology and Services Supply Chain", *White House*, 15.května 2019, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/(přístup 17.prosince 2023)

[72] Cecilia Kang a David E. Sanger, „Huawei Is a Target as Trump Moves to Ban Foreign Telecom Gear." *The New York Times*, 15.května 2019, https://www.nytimes.com/2019/05/15/business/huawei-ban-trump.html. (staženo 19.listopadu 2023).

[73] David Shepardson a Karen Freifeld, „China's Huawei, 70 Affiliates Placed on U.S. Trade Blacklist ." *Reuters*, 16.května, 2019. https://www.reuters.com/article/us-usa-china-huaweitech-idUSKCN1SL2W4/.(staženo 19.listopadu 2023).

[74] Jon Bateman , *U.S.-China Technological "Decoupling": A Strategy and Policy Framework, (*Washigton D.C : Carnegie Endowment for International Peace, 2022),29-30, https://carnegieendowment.org/files/Bateman_US-China_Decoupling_final.pdf (staženo 11.listopadu 2023).

[75] Hadi Chapardar, William X. Wei, a Houssam Chamseddine „ Huawei in Canada: Doing business in the midst of Game of Thrones" in in *Huawei Goes Global: Volume II: Regional, Geopolitical Perspectives and Crisis Management,* ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann, (London: Palgrave Macmillan, 2020), 132.

mohly zvážit možnost postihu.[76] V květnu 2020 Spojené státy zpřísnily své kontroly vývozu, a nově vyžadovaly licenci pro prodej mikročipů společnosti Huawei, dokonce i zahraničních výrobků vyrobený pomocí americké technologie.[77]

3.3 Světový zákaz společnosti Huawei

Americká vláda požádala své spojence, aby zakázali používání technologií 5G společnosti Huawei. Ministr zahraniční USA Michael Pompeo zdůraznil v rozhovoru pro *Fox Business Network*, že v uplynulých měsících americká vláda aktivně spolupracovala se zeměmi po celém světě, aby je informovala o rizicích spojených se začleněním technologií Huawei do tamních telekomunikačních systémů. Zdůraznil, že je důležité si uvědomit, že tyto systémy byly navrženy ve spolupráci s čínskou armádou a ohrožují nejen bezpečnost dotčených zemí, ale také blaho jejich obyvatele.[78] Přesto se ukázalo, že varování přiměla pouze několik vlád, aby následovaly americkému příkladu a zakázaly Huawei.

Spojené království za vlády Theresy Mayové i Borise Johnsona nejprve udělilo společnosti Huawei povolení k výstavbě sítě 5G v zemi. V červenci 2020 však Johnsonova vláda svůj postoj náhle změnila a rozhodla se zakázat společnosti Huawei účast na síti 5G a vyzvala národní telekomunikační poskytovatele, aby do konce roku 2027 odstranili zařízení Huawei ze svých sítí 5G. Podle britských médií prý premiér Johnson osobně informoval společnost Huawei o tom, že jeho rozhodnutí zakázat účast firmy v síti 5G bylo motivováno geopolitickým tlakem ze strany administrativy prezidenta Trumpa. Johnson také údajně uvedl, že pokud USA v budoucnu změní svou politiku vůči Číně, bude stále možné, aby Spojené království znovu zvážilo účast společnosti Huawei na budování sítě 5G v zemi.[79]

V září 2019 Polsko a USA podepsaly společné prohlášení o posílení spolupráce v oblasti 5G a zdůraznily důležitost volné hospodářské soutěže, transparentnosti a právního státu při budování

[76] Ana Swanson, „U.S. Delivers Another Blow to Huawei with New Tech Restrictions." *The New York Time*s, 15.května 2020, https://www.nytimes.com/2020/05/15/business/economy/commerce-department-huawei.html.
[77] Keman Huang, Stuart Madnick, Fang Zhang a Michael Siegel, „Varieties of public–private co-governance on cybersecurity within the digital trade: implications from Huawei's 5G," *Journal of Chinese Governance* 7, č. 1 (2022): 97, https://doi.org/10.1080/23812346.2021.1923230 (staženo 19.listopadu 2023).
[78] Mike Pompeo, interview vedla Maria Bartiromo, *Mornings With Maria,* Fox Business Network, 6.února 2019, https://2017-2021.state.gov/interview-with-maria-bartiromo-of-mornings-with-maria-on-fox-business-network-2/
[79] Pak Nung Wong, *Techno-Geopolitics: U.S.-China Tech War and the Practice of Digital Statecraft*, 52.

sítě 5G.[80] Tím obě země implicitně vyjádřily obavy ohledně možných rizik spojených s účastí společnosti Huawei. Podobná deklarace o bezpečnosti sítí 5G byla později podepsána českým premiérem Andrejem Babišem a americkým ministrem zahraničí Mikem Pompem.[81] Naopak, bývalá německá kancléřka Merkelová zvolila opačný přístup a spíše než výslovné zákazy pro jednotlivé společnosti, upřednostnila obecnější zpřísnění bezpečnostních požadavků pro všechny účastníky programu 5G, bez ohledu na jejich původ.[82]

4. Rozhodnutí zakázat společnost Huawei

4.1 Huawei jako hrozba pro kybernetickou bezpečnost

Když v květnu roku 2019 Trump zakázal společnost Huawei na americkém trhu, uvedl, že zahraniční odpůrci zneužívají slabin v informačních a komunikačních technologiích, které pak mohou vyústit v nebezpečné kybernetické operace, včetně průmyslových špionáží proti Spojeným státům.[83] Podezření vycházelo z celkových aktivit Číny v kyberprostoru. Soubor dat o kybernetických incidentech a kampaních (*The Dyadic Cyber Incident Dataset*) určil Čínskou lidovou republiku jako hlavního globálního viníka kybernetické špionáže, přičemž čínské aktivity jsou o 30 % častější než ty ruské.[84] Podobná zjištění nabízí i databáze Rady pro zahraniční vztahy (*Council on Foreign Relations*), která dokumentuje veřejně známé státem podporované kybernetické incidenty od roku 2005 až do současnosti. Tato databáze přisuzuje Číně odpovědnost za 290 incidentů, což ji činí nejčastěji zmiňovaným sponzorem kybernetických operací.[85]

[80] Paulina Uznaska, „Will Poland Be an Anti-Huawei Force in the EU?" *The Diplomat*, 27.srpna 2020. https://thediplomat.com/2020/08/will-poland-be-an-anti-huawei-force-in-the-eu/(staženo 19.prosince 2023)
[81] ČTK, „Přispěje K Národní Bezpečnosti." Babiš Podepsal S Americkým Ministrem Zahraničí Deklaraci O 5g Sítích." *iROZHLAS*, 6. května 2020. https://www.irozhlas.cz/veda-technologie/technologie/andrej-babis-mike-pompeo-5g-mobilni-site-dodavatele-usa-cesko_2005062234_dok. (staženo 19.prosince 2023).
[82] Rebecca Staudenmaier, „ German Minister Warns of 5G Delays If Huawei Is Left out", *Deutsche Welle* 18.ledna 2020. https://www.dw.com/en/germanys-seehofer-warns-of-5g-delays-if-huawei-is-excluded/a-52050565. (staženo 19.prosince 2023).
[83] Donald J. Trump, „ Executive Order on Securing the Information and Communications Technology and Services Supply Chain", *White House*, 15.května 2019, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing- information-communications-technology-services-supply-chain/(přístup 17.prosince 2023).
[84] Benjamin Jensen, „ How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy." *CSIS*, 19.října 2023, https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy. (přístup 7. prosince 2023)
[85] „Cyber Operation Tracker ", *Council on Foreign Relations*, https://www.cfr.org/cyber-operations/ (přístup 7.prosince 2023)

Čínské kybernetické špionáže

Čínské kybernetické operace jsou obvykle strategického charakteru a prováděné skupinami kybernetických útočníků, kteří využívají propracovaných metod k proniknutí do cílových sítí. Jejich hlavním cílem je setrvat nepozorovaně v těchto sítích co nejdéle a systematicky shromažďovat informace.[86] Čínská strategie klade velký důraz na dosažení informační převahy nad USA. Tímto způsobem může Čína lépe porozumět vojensko-strategickým schopnostem USA a využít tyto poznatky k modernizaci čínské armády.[87]

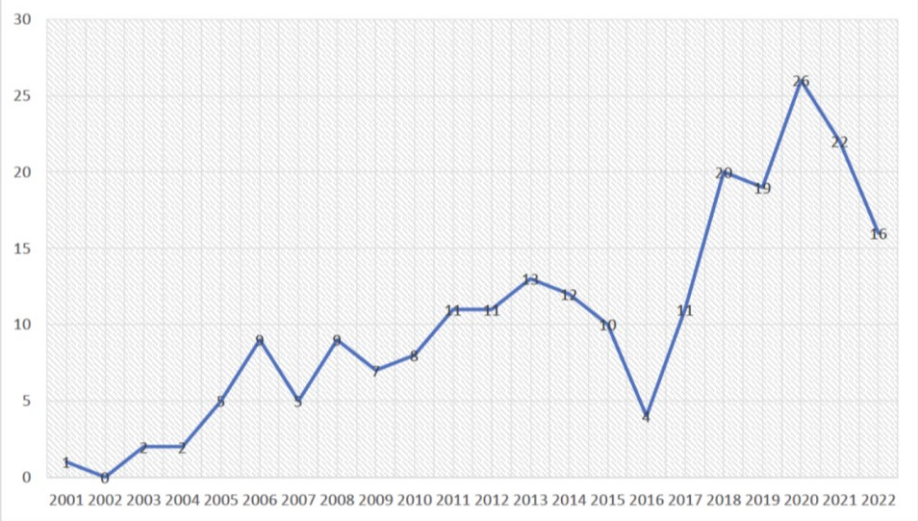
Případ Su Bina z roku 2014 slouží jako ilustrativní příklad těchto čínských snah. Číňan Su Bin byl obviněn a následně uznán vinným z účasti na kybernetické špionáži, kterou prováděli hackeři z Lidové osvobozenecké armády Číny.[88] Cílem této špionáže bylo získání důležitých dat od amerických obranných dodavatelů, jako jsou společnosti Lockheed Martin a Boeing, jelikož se podílejí na vývoji a výrobě vojenského letectva. Su Bin instruoval čínské hackery, určoval jejich cíle a překládal získaná data. Tento incident ukázal přímé zapojení čínského občana do kyberšpionáže na pokyn čínské vlády. Ukradené informace umožnily Čínské lidové republice provést důkladnou analýzu a aplikaci reverzního inženýrství na komponenty amerických vojenských letadel, čímž dosáhla efektivní úspory času a finančních prostředků, které by jinak musela investovat do vlastního výzkumu a vývoje těchto technologií.[89]

Dokonce i samotná federální vláda se stala cílem čínských kybernetických útoků, jak ukazuje útok na *Office of Personnel Management* (OPM). Během tohoto útoku byla OPM ukradena citlivá osobní data více než čtyřem milionů zaměstnanců federální vlády a žadatelů o víza do Spojených států.[90] Kromě vojenských a politických informací je pro Čínu důležité získávat i obchodní tajemství. Kybernetická špionáž, jak uvádí Národní centrum kontrarozvědky a bezpečnosti, může ohrozit dlouhodobou ekonomickou převahu Spojených států, jelikož probíhá

[86] Jason R. Fritz, *China's Cyber Warfare: The Evolution of Strategic Doctrine,* 71.
[87] Brandon Valeriano, " China and the Technology Gap: Chinese Strategic Behavior in Cyberspace", in *Cyber Strategy: The Evolving Character of Power and Coercion*, 158–162.
[88] Office of Public Affairs, „Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information", 23.května 2016, https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive(přístup 12.prosince 2023).
[89] Deborah Kidwell, „Cyber Espionage for the Chinese Government." *Office of Special Investigations,* 17.září 2020. https://www.osi.af.mil/News/Features/Display/Article/2350807/cyber-espionage-for-the-chinese-government/(přístup 12.prosince 2023).
[90] Magdalena Fiřtová, Jan Hornát a Jana Sehnálková (eds.), Prezidentství Baracka Obamy: naplněné vize?, 225.

ve skoro všech klíčových odvětvích země, včetně energetiky, biotechnologie a technologie.[91] Právě v květnu 2014 obvinilo Ministerstvo spravedlnosti Spojených států pět důstojníků čínské armády z kybernetické špionáže a krádeže obchodních tajemství od amerických společností v solárním a ocelářském odvětví, které sama čínská vláda označuje za zásadní pro vlastní ekonomický růst.[92]

Otázka kybernetických útoků byla proto jedním z hlavních témat čínsko-amerických summitů za Obamovy administrativy. Washington začal intenzivně prosazovat tuto záležitost v rámci diplomatických jednání i veřejně.[93] Během summitu prezidentů Obamovy a Si Ťin-pchinga v září 2015 se obě strany dohodly, že „vláda žádné z obou zemí nebude provádět nebo vědomě podporovat kybernetické krádeže duševního vlastnictví, obchodních tajemství nebo jiných důvěrných obchodních informací, a že se bude snažit zabránit jejich zneužití".[94]



Graf 2: Počet zaznamenaných čínských špionážní aktivit v USA (2000-2022), zdroj: CSIS

[91] National Counterintelligence and Security Center, „ Foreign Economic Espionage in Cyberspace," 2018, 11, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf (staženo 7.prosince 2023).
[92] Manshu Xu a Chuanying Lu, China–U.S. cyber-crisis management, *China International Strategy Review* 3, 105 (28.června 2021). https://doi.org/10.1007/s42533-021-00079-7 (staženo 7.prosince 2023).
[93] Magdalena Fiřtová, Jan Hornát a Jana Sehnálková (eds.), Prezidentství Baracka Obamy: naplněné vize? (Praha: Karolinum, 2017), 225.
[94] Everett Rosenfeld, „US-China Agree to Not Conduct Cybertheft of Intellectual Property." *CNBC*, 25.září 2015, https://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html. (staženo 13.dubna 2024).

Z analýzy grafu 2 vyplývá, že po roce 2015 došlo k výraznému snížení čínských špionážních aktivit.[95] Navzdory tomu však došlo po nástupu Donalda Trumpa do prezidentského úřadu ke zvýšení těchto aktivit ze strany Číny, především v roce 2018, kdy byl zaznamenán jejich výrazný nárůst. Během Trumpovy administrativy se vztahy mezi Spojenými státy a Čínou zhoršily, především kvůli obchodní válce, jež mohla vyprovokovat odvetné kybernetické akce. V této situaci, kdy zřejmě nedošlo k plnému dodržování kybernetické dohody z roku 2015, se Trumpova administrativa mohla cítit povinna zasáhnout a chránit národní kybernetickou bezpečnost USA, což mohlo následně vést k omezení činnosti společnosti Huawei na americkém trhu. Administrativa Donalda Trumpa jednající jako racionální aktér v hodnocení situace, dospěla tedy k závěru, že bezpečnostní rizika spojená s čínskou společností Huawei převyšují její potenciální ekonomické přínosy.

Podle Trumpovy administrativy se Čína zapojila do rozsáhlé kybernetické hospodářské špionáže a krádeží duševního vlastnictví, přičemž hodnota těchto nelegálních aktivit dosahovala „několika miliard dolarů''.[96] V roce 2018 se americká vláda rozhodla uvalit cla na čínské zboží, včetně technologických produktů, s odůvodněním, že tak reaguje na zjištění Úřadu obchodního zástupce Spojených států (USTR). Podle tohoto vyšetřování čínská vláda údajně prováděla nekalé praktiky, včetně podpory nebo iniciování kybernetických útoků zaměřených na americké komerční sítě, s cílem získat důvěrné obchodní informace držené americkými firmami.[97]

Huawei a zadní vrátka

Americký ministr zahraničí Mike Pompeo a viceprezident Mike Pence varovali, že zařízení čínské společnosti Huawei mohou obsahovat zadní vrátka.[98] Tyto skryté průchody by tedy mohla čínská vláda využít pro špionážní účely. Právě nizozemský deník *De Volkskrant*

[95] „ Survey of Chinese Espionage in the United States Since 2000'', Center for Strategic and International Studies, březen 2023, https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000, (přístup 23.prosince 2023).
[96] The White House, „National Cyber Strategy of the United States America ", září 2018, 2, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (staženo 7.prosince 2023).
[97] Office of the United States Trade Representative, „China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation" , 22.března 2018, 171-172 https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF, (staženo 7.prosince 2023),.
[98] Briefing, „ Huawei Is at the Centre of Political Controversy." *The Economis*t, 27. dubna 2019. https://www.economist.com/briefing/2019/04/27/huawei-is-at-the-centre-of-political-controversy.

informoval na základě nejmenovaných zdrojů rozvědky, že telekomunikační vybavení společnosti Huawei obsahuje tato zadní vrátka, která firmě mohla umožnit neoprávněný přístup k datům svých zákazníků. Při hodnocení rizika v oblasti kybernetické bezpečnosti používají forenzní odborníci škálu od jedné do deseti, kde jednička představuje minimální riziko a desítka označuje kritické riziko. Podle experta na kybernetickou bezpečnost Pavola Luptáka kritické riziko znamená, že útočník může získat úplnou kontrolu nad daným zařízením, aniž by to vlastník zjistil. Téměř 27 % zařízení od společnosti Huawei prokázala kritické množství bezpečnostních slabostí. [99]

Je důležité zdůraznit, že Spojené státy také realizují kybernetickou špionáž proti Čínské lidové republice. Podle informací *New York Times* Národní bezpečností agentura (NSA) pronikla do serverů Huawei, aby získala citlivé údaje a sledovala komunikaci vrcholných manažerů firmy. Operace „Shot Giant", kterou odhalil whistleblower Edward Snowden, měla za cíl získat politické informace o spojení mezi společností Huawei a Komunistickou stranou Číny. Dalším záměrem bylo získat zdrojové kódy produktů Huawei pro možné využití ve špionážních operacích.[100] Díky této operaci mohly Spojené státy monitorovat komunikaci v „nepřátelských'' zemích USA, používajících Huawei technologie, jako je Írán, Afghánistán, Pákistán, Keňa a Kuba. Ze získaných dat však nevyplývá, zda Huawei působí nezávisle nebo jestli je nástrojem čínské armády.[101]

Celkově nebyl nikdy předložen ze strany Spojených států žádný důkaz o špionážních prvcích v Huawei produktech. Rozsáhlá 18měsíční bezpečnostní prověrka amerických vládních agentur v roce 2012 dospěla k závěru, že neexistují žádné důkazy, usvědčující společnost Huawei ze spolupráce s čínskou vládou na špehování občanů Spojených států. Stejně tak zpráva Výboru pro zpravodajské služby Sněmovny reprezentantů, které varovala americké telekomunikační společnosti před obchodováním se společností Huawei, neposkytla prakticky žádné důkazy o bezpečnostní hrozbě, jež měla představovat čínská telekomunikační společnost.[102] Je ale

[99] Pavla Holcová, „Co Je Špatně (s) Huawei?!" *investigace.cz*, 29.října 2019, https://www.investigace.cz/co-je-spatne-s-huawei/.
[100] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, 40.
[101] David E. Sanger a Nicole Perlroth, „N.S.A. Breached Chinese Servers Seen as Security Threat." T*he New York Times*, 22.března 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html. (staženo 7.prosince 2023).
[102] Denise Tsang a David Luigi Fuschi, „A Strategic Assessment of Huawei into the Fast Future" in *Huawei Goes Global: Volume I: Made in China for the World*, 134-135.

možné, že vzhledem k důvěrnosti informací nemohla americká vláda zveřejnit konkrétní důkazy o spojení Huawei s čínskou vládou. Jak Bolton sám řekl, Huawei představovala obrovské bezpečnostní riziko, jenž nebylo možné sdělit veřejnosti.[103]

Dva zákony přijaté v Číně, týkající se ochrany dat, však znepokojily mezinárodní společnost. Zákon o národních zpravodajských službách z roku 2017 uvádí, že všechny organizace a občané, včetně společností jako je Huawei, musí podporovat, pomáhat a spolupracovat se státními zpravodajskými službami, když to vyžaduje zákon.[104] Zákon o kontrašpionáži z roku 2014 rovněž tvrdí, že organizace a jednotlivci nesmí takovou žádost odmítnout. To znamená, že i když Huawei tvrdí, že působí nezávisle a neohrožuje zájmy svých klientů, může být vystavena vládnímu tlaku, vzhledem k povaze nedemokratického politického systému v Čínské lidové republice.[105] Nasazení 5G sítí společnosti Huawei v USA představovalo pro administrativu vážný bezpečnostní problém, vzhledem k historii čínských kyber špionážních incidentů mířených proti Spojeným státům a samotná společnost čelila obviněním z možné špionáže a nerespektování amerických sankcí vůči Íránu.

S ohledem na potenciální bezpečnostní rizika spojená s technologiemi 5G od společnosti Huawei, USA aktivně vybízely své spojence k přijímání podobných bezpečnostních opatření, s cílem omezit používání technologií této společnosti. Trumpova kybernetická strategie kladla důraz na koordinaci a jednotné postupy v oblasti kybernetické bezpečnosti mezi spojenci, nezbytných pro vytvoření účinného systému obrany proti globálním kybernetickým hrozbám. Pokud by se spojenecká země rozhodla vybudovat svou 5G síť pomocí zařízení od společnosti Huawei, mohla by tím ohrozit výměnu informací a zpravodajskou spolupráci se Spojenými státy.[106]

[103] John Bolton, *The Room Where It Happened*, 185.
[104] Department of Homeland Security, „ 5G Impacts on Cybersecurity “, 28. září 2023, https://www.dhs.gov/sites/default/files/2023 09/23_0906_oia_01_5G_Security_508_Compliant.pdf (staženo 7.prosince 2023).
[105] Manshu Xu a Chuanying Lu, „China–U.S. cyber-crisis management“, *China International Strategy Review* 3, 105 (28.června 2021). https://doi.org/10.1007/s42533-021-00079-7 (staženo 7.prosince 2023).
[106] Joe Gol, „Esper to Allies: Picking Huawei Risks Intel and Security Ties with the US.” *Defense News,* 15 února 2020. https://www.defensenews.com/congress/2020/02/15/esper-huawei-5g-could-risk-us-information-and-security-ties/, (staženo 7.prosince 2023).

Trumpův postoj ke kybernetické bezpečnosti

Otázkou ale zbývá, jak Trump skutečně vyhodnocoval kybernetická rizika spojená se společností Huawei. Během své prezidentské kampaně Trump prohlásil, že bývalý prezident Barack Obama umožnil Číně provádět kybernetické útoky za účelem krádeže státních tajemství a provozovat průmyslovou špionáž proti Spojeným státům a jejich společnostem.[107] Trump měl také během svého mandátu tendenci často připisovat Číně odpovědnost za různé kybernetické útoky, i když jasné důkazy tvrdily opak. V případě útoku na Demokratický národní výbor (DNC) naznačoval Trump, že za něj mohla být zodpovědná Čína, i když dostupné důkazy jednoznačně směřovaly k Rusku, jako hlavnímu pachateli tohoto kybernetického útoku.[108] Trump mohl mít svá osobní přesvědčení o permanentní zapojenosti Číny do kyberšpionáže a toto přesvědčení mohlo být hlavním motivem pro jeho rozhodnutí zakázat činnost společnosti Huawei v USA. Nicméně, pravděpodobnější je, že Trump chtěl odvrátit pozornost od ruského vměšování do voleb[109] , tím, že by vinu za kybernetické útoky přisoudil Číně.

Mimo jiné Trump často přicházel s alternativními teoriemi, například při úniku dat z firmy SolarWinds v roce 2020. Tehdy tvrdil, že zpravodajství o kybernetickém útoku bylo přehnané a kritizoval média za zaměření se na Rusko místo na možnou roli Číny. Bez důkazů naznačil možnou manipulaci s hlasovacími zařízeními během voleb a tvrdil, že tyto nekalé praktiky přispěly k jeho porážce. Jeho tvrzení bylo v rozporu s oficiálním stanoviskem generální prokurátora William Barra a ministra zahraničí Mika Pompea, kteří SolarWinds útok jednoznačně přisoudili Rusku.[110] Bývalý americký prezident měl tedy tendenci vyjadřovat

[107] Alice Rezková, „ Čínská karta v amerických prezidentských volbách“ v ‘‘ America First Příčiny a kontext volebního vítězství Donalda Trumpa, ed, Jan Hornát a Lucie Kýrová (Praha : Karolinum, 2020), 230-231.
[108] Andy Greenberg „Trump’s Worst, Most Bizarre Statements about ‘The Cyber‘‘, *Wired*, 18.ledna 2021. https://www.wired.com/story/trump-cyber-worst-quotes-statements-hackers-ukraine-russia/. (staženo 23.12.2023)
[109] Eric Geller. “Mueller’s Timeline: How the Russian Hacks Unfolded - Politico.” Politico , July 13, 2018. https://www.politico.com/story/2018/07/13/mueller-russia-hacks-timeline-686521.
[110] Veronica Stracqualursi, „ Kevin Liptak, a Jennifer Hansler, „Trump Downplays Massive Cyber Hack on Government after Pompeo Links Attack to Russia“ , *CNN*, 19.prosince 2020, https://edition.cnn.com/2020/12/19/politics/pompeo-us- government-hack-russia/index.html.

pochybnosti ohledně závažnosti kybernetických hrozeb a často se vyhýbal přijímání oficiálních zpravodajských zjištění týkajících se těchto hrozeb.[111]

V otázce kybernetické bezpečnosti 5G sítí, podle Toma Wheelera, zasedajícího ve Federální komunikační komisi (FCC) v období 2013-2017, zastavila administrativa prezidenta Trumpa snahy začlenit kybernetickou bezpečnost jako nedílnou součást standardu pro 5G a vytvořit tak bezpečností standardy před samotnou výstavbu sítě, iniciované již během Obamovy administrativy. Dále také odmítla varování Národního bezpečnostní rady (NSC) týkající se kybernetické bezpečnosti v 5G síti. Kongres se proto rozhodl aktivně zasáhnout do věci kvůli nedostatečné iniciativy Trumpovy administrativy. Bipartitní vedení Výboru pro energetiku a obchod Sněmovny reprezentantů napsalo v květnu předsedovi FCC Ajitovi Paiovi, že kybernetická bezpečnost 5G „si zaslouží, aby se na ni agentura výslovně zaměřila a věnovala jí větší pozornost."[112] Až po té, co Kongres pověřil Trumpovu administrativu vypracováním národní strategie pro využití technologie 5G v rámci zákona NDAA 2020,[113] Trumpova administrativa konečně předložila svoji kybernetickou strategii ohledně technologie 5G.

4.2 Huawei jako hrozba pro americkou technologickou dominanci

Vyloučení společnosti Huawei z amerických 5G sítí může být považováno za racionální krok, zejména vzhledem k obavám USA o kybernetickou bezpečnost. Na druhou stranu, rozhodnutí Trumpovy administrativy zakázat americkým společnostem dodávat software a polovodičové komponenty společnosti Huawei podle většiny expertů na kybernetickou bezpečnost z ankety „The Cybersecurity 202" v deníku *The Washington Post* pravděpodobně nezvýší americkou bezpečnost. Odborníci varovali, že tento zákaz může mít negativní dopad na americké technologické společnosti, jelikož přicházejí o důležitého obchodního partnera. Současně může omezení spolupráce s Huawei snížit vliv USA na vytváření bezpečnostních standardů a regulací v oblasti nových technologií. Jiní se obávali, že Čína vytvoří svůj domácí technologický

[111] Andy Greenberg, „Trump's Worst, Most Bizarre Statements about 'The Cyber'', *Wired*, 18.ledna 2021. https://www.wired.com/story/trump-cyber-worst-quotes-statements-hackers-ukraine-russia/. (staženo 23.12.2023)
[112] Tom Wheeler, „5G in Five (Not So) Easy Pieces." Brookings Institution, 9.července 2019, https://www.brookings.edu/articles/5g-in-five-not-so-easy-pieces/
[113] Congress „NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2020'', 73, 20.prosince 2019 , https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf (staženo 17.dubna 2023).

průmysl, aby snížila závislost na amerických dodavatelích.[114] Achillovou patou Číny je onen design polovodičových čipů, kde Spojené státy fakticky drží monopol.[115] Huawei, jež nedávno ještě využívala americké čipy k výrobě svých smartphonů a telekomunikačních zařízení, se dostala do značně obtížné situace.

Zařazení společnosti Huawei na seznam subjektů ministerstva obchodu bylo strategickým krokem s cílem dosáhnout celosvětového zákazu této čínské společnosti. Rozhodnutí bylo učiněno, protože Trumpova administrativa neuspěla v diplomatických jednáních při přesvědčování svých spojenců k hromadnému odmítnutí společnosti Huawei při nasazování 5G sítí. Nařízení amerického ministerstva obchodu má totiž také extrateritoriální rozsah, neboť se vztahuje i na zboží zahraničního původu. Přestože výrobky mohou být vyrobeny nebo navrženy mimo území Spojených států, obsahují-li nebo využívají-li technologie pocházející z USA, může americká vláda, prostřednictvím Ministerstva obchodu, omezit jejich dovoz do společnosti Huawei.

Bylo zřejmé, že zákaz Huawei má na americké společnosti negativní dopad. V reakci na to Trumpova administrativa později umožnila společnosti Huawei nadále nakupovat polovodiče a další zboží z USA a ze zahraničí. Avšak license určené pro čipy na vývoj 5G systémů byly okamžitě odmítnuty americkou vládou.[116] Je tedy jasné, že se Trumpova vláda snažila ochromit schopnost společnosti Huawei ve vývoji a zavádění pokročilé telekomunikační infrastruktury 5G. Donald Trump sám poznamenal o technologii 5G: „Nemůžeme dovolit, aby nás jakákoliv jiná země překonala v tomto mocném průmyslu budoucnosti. Závod o 5G je závod, který Amerika musí vyhrát.“[117]

---

[114] Joseph Marks „ The Cybersecurity 202: Trump's ban on U.S. companies supplying Huawei will not make the country safer experts say'', *The Washigton Post*, 4.června 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/06/04/the-cybersecurity-202-trump-s-ban-on-u-s-companies-supplying-huawei-will-not-make-the-country-safer-experts-say/5cf5c40ba7a0a46b92a3ff86/(staženo 17.prosince 2023).

[115] Frank Tang a Ji Siqi. „Starved of Chips, China faces 'unprecedented' pressure to become No 1 Economy." *South China Morning Post*, 13.dubna 2023. https://www.scmp.com/economy/china-economy/article/3209385/tech-war-starved-semiconductors-chinas-bid-topple-us-no-1-economy-faces-unprecedented-pressure.

[116] Jon Bateman , *U.S.-China Technological "Decoupling": A Strategy and Policy Framework, (*Washigton D.C : Carnegie Endowment for International Peace, 2022), 37.

[117] Donald Trump, „ Remarks by President Trump on United States 5G Deployment", 12.dubna 2019, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/ (přístup 19. prosince 2023)

Vládní zákaz vůči společnosti Huawei můžeme chápat jako součástí širšího plánu, která má omezit čínský technologický pokrok a zachovat americké vedení v technologiích. Tato strategie je právě v souladu s Trumpovou Národní bezpečnostní strategií, která klade důraz na udržení americké vedoucí pozice v oblastech inovací a výzkumu.[118] Dále Kongres v roce 2018 schválil Zákon o reformě kontroly exportu (*Export Control Reform Act*), který prohlašuje, že americká národní bezpečnost „vyžaduje, aby Spojené státy udržely své vedení ve vědeckých, technologických, inženýrských a výrobních sektorech, včetně základních technologií, které jsou nezbytné pro inovace“. Z důvodu obav z technologického pokroků Číny byl proto zákon schválen.[119]

Čínský technologický růst

V posledních dvou desetiletích se technologický ekosystém mezi USA a Čínou hluboce propojil, protože se čínská ekonomika silně integrovala se Západem. Oba hráči těžili z globálních technologických řetězců, které zvyšovaly výrobu a efektivitu nákladů. Nicméně se zdálo, že Čína těžila z této spolupráce více, jelikož role čínských společností v celosvětové výrobě a vývozu informačních a komunikačních technologií rychle rostla. Do roku 2019 dosahovala přibližně až 40 %.[120] Právě během Trumpovy éry byla Čína označena za hlavního strategického rivala Spojených států.[121] Tento krok, uznávající rostoucí sílu Čínské lidové republiky, vedl v březnu 2018 k zahájení obchodní války a vyhlášení vysokých cel na čínský dovoz oceli a hliníku, ačkoliv to bylo v rozporu s pravidly Světové obchodní organizace. Trumpova opatření byla ospravedlnitelná jako nezbytná k zajištění národní bezpečnosti Spojených států.[122] Obchodní válka s Čínou se neomezovala pouze na cla, ale došlo k posílení kontroly nad čínskými vědeckými a technologickými aktivitami v USA. Začala se propagovat

[118] United States of America, *National Security Strategy of the United States of America*, prosinec 2017, 41, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (staženo 13.prosince 2023).
[119] Jon Bateman , *U.S.-China Technological "Decoupling": A Strategy and Policy Framework, (*Washigton D.C : Carnegie Endowment for International Peace, 2022), 5.
[120] Paul Evans. "Techno-nationalism in China–US Relations: Implications for Universities." *East Asian Policy 12*, č. 2 (2020): 85.
[121] Aiden Warren a Adam Bartley, *US Foreign Policy and China: The Bush, Obama, Trump Administrations (*Edinburgh: Edinburgh University Press, 2020), 160.
[122] Wong, *Techno-Geopolitics: U.S.-China Tech War and the Practice of Digital Statecraft*, 6.

strategii tzv. decouplingu, což znamená proces oddělování amerického technologického sektoru od čínského, s cílem zabránit dalšímu rozvoji čínských technologií ve Spojených státech.[123]

Zájem americké vlády o technologický decoupling lze vysvětlit dvěma hlavními trendy.[124] Za prvé, dochází ke změně rétoriky amerických politiků vůči Číně. Ještě na začátku 21. století ve Washingtonu převažoval názor, že vzestup Číny je v souladu s americkými zájmy. Právě v roce 2005 Robert Zoellick, tehdejší náměstek ministra zahraničí, vyzval Peking, aby se stal „zodpovědným podílníkem" (responsible stakeholder) a zapojil se do řešení mezinárodních otázek. V důsledku různých katalyzátorů se tento konsenzus se začal rozpadat, jako příklad lze uvést modernizace Čínské lidové armády, čínské aktivity v Jihočínském moři, krádeže intelektuálního vlastnictví a porušování lidských a politických práv v Číně. Ukázalo se tedy, že se Čína chová spíše jako neochotný spolupodílník (reluctant stakeholder) a v některých případech se snaží stanovené mezinárodní normy podkopávat.[125]

Za druhé, americký proces oddělování se od čínských produktů je spojen s konceptem techno-nacionalismu. Techno-nacionalisté zdůrazňují technologickou nezávislost jako klíčový prvek národní bezpečnosti. Podle nich je schopnost země vytvářet a ovládat klíčové technologie klíčová pro ochranu vlastní suverenity. Důležitou součástí této strategie je rozvoj domácího průmyslu a inovací, aby země nebyla závislá na importu technologií ze zahraničí. [126]

Právě Čína prosazovala politiku techno-nacionalismu například již zmíněnou iniciativou „Made in China 205". Nový čínský program vyvolal značné napětí ve Spojených státech. V červnu v roce 2018 americký obchodní zmocněnec Robert Lighthizer obvinil čínskou vládu z toho, že „agresivně podkopává americké vyspělé technologické průmysly a ekonomické vedení prostřednictvím nespravedlivých obchodních praktik a průmyslových politik, jako je plán „Made in China 2025".[127] Necelé čtyři měsíce po tomto prohlášení viceprezident Mike

---

[123] Jon Bateman , *U.S.-China Technological "Decoupling": A Strategy and Policy Framework, (*Washigton D.C : Carnegie Endowment for International Peace, 2022), 5, https://carnegieendowment.org/files/Bateman_US-China_Decoupling_final.pdf (staženo 11.listopadu 2023).

[124] Jon Bateman , *U.S.-China Technological "Decoupling": A Strategy and Policy Framework, (*Washigton D.C : Carnegie Endowment for International Peace, 2022), 5.

[125] Magdalena Fiřtová, Jan Hornát a Jana Sehnálková (eds.), Prezidentství Baracka Obamy: naplněné vize? 240.

[126] Pak Nung Wong, *Techno-Geopolitics: U.S.-China Tech War and the Practice of Digital Statecraft*, 52.

[127] United States Trade Representative (USTR). "USTR Issues Tariffs on Chinese Products in Response to Unfair Trade Practices." Press Release, 15. června 2018. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/june/ustr-issues-tariffs-chinese-products.

Pence zesílil kritiku Spojených států ve svém projevu v Hudsonově institutu: „Nyní si Komunistická strana prostřednictvím plánu ,,Made in China 2025‘‘ klade za cíl ovládnout 90 % světových nejvyspělejších průmyslových odvětví“.[128]

Trumpova administrativa se výrazně posunula směrem k přijímání myšlenek techno – nacionalismu (a celkově i nacionalismu) v rámci americké strategie a značně rozšířila opatření zaměřených na řešení hrozeb ze strany čínských technologií. Americká techno-nacionalistická politika se často dělí na dvě skupiny. Cílem „defenzivních" opatření je zmařit a omezit technologické hrozby ze strany Číny, zatímco „ofenzivní" opatření se snaží posílit vlastní technologickou sílu Ameriky. Během Trumpovy éry se politici v administrativě a Kongresu v drtivé většině zaměřili na defenzivní opatření, například kontroly vývozu, omezení čínských investic a zamítnutí víz a regulačních licencí pro čínské pracovníky, studenty a čínské podniky.[129]

Technologický náskok je pro Spojené státy zásadní, jelikož přispívá k jejich hospodářské prosperitě a umožňuje jim udržet si vojenskou a ekonomickou převahu. Rozvoj Číny v oblasti páté generace bezdrátových sítí by tak mohl opakovat úspěch, podobný tomu, dosaženému Spojenými státy v éře čtvrté generaci. V období 4G LTE technologie skutečně dominovaly Spojené státy, především díky rychlému přijetí a rozšíření sítě, zatímco v éře 3G měly větší vliv evropské firmy. Rozvoj 4G LTE výrazně přispěl k rozvoji tzv. sdílené ekonomiky a vedl k vzestupu společností jako Lyft, Uber a Airbnb.[130] Podle analýzy společnosti Deloitte, pokud by Spojené státy přišly o své vedoucí postavení v mobilním průmyslu, mělo by to negativní dopady nejen na tyto sektory, ale také na celou americkou ekonomiku, protože více závisí na mobilních službách, které jsou využívány jak spotřebiteli, tak podniky.[131]

[128] Hudson Institute. 2018. "Vice President Mike’s Remarks on the Administration’s Policy Towards China." 4.října https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018.
[129] Jon Bateman , *U.S.-China Technological “Decoupling”: A Strategy and Policy Framework, (*Washigton D.C : Carnegie Endowment for International Peace, 2022), 37.
[130] Nicol Turner Lee, „Navigating the U.S.-China 5G Competition", *GLOBAL CHINA, Brookings Institution*, 3-5 https://www.brookings.edu/articles/navigating-the-us-china-5g-competition/.
[131]Deloitte, ,, United States expands global lead in mobile broadband‘‘, září 2014, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-mobile-index-09262014.pdf (staženo 12. prosince 2023).

Prezident Trump se osobně angažoval v jednáních s americkými manažery telekomunikačních firem o vývoji technologie 5G a zvažoval různé verze výkonného nařízení. Během těchto setkání ale mu bylo brzy řečeno, že žádné americké společnosti nemohou konkurovat Huawei v systému 5G. Je tedy nepravděpodobné, že Spojené státy „vyhrají" závod ve vývoji 5G.[132] Nicméně pro Spojené státy bylo důležité, aby zastavily čínský růst v oblasti 5G kvůli jejímu strategickému významu. Pokud by si Čína měla udržet své vedoucí postavení v 5G technologiích, mohlo by to vést k tomu, že se celosvětový digitální průmysl přeorientuje směrem k Číně. Spojené státy dokázaly prozatím zastavit růst čínské společnosti v oblasti 5G. Podíl společnosti Huawei na celosvětovém trhu se zařízeními 5G rychle klesá. V roce 2018 měla společnost Huawei díky obrovským technologickým a cenovým výhodám ve srovnání s ostatními konkurenty velký náskok v zakázkách 5G a zaujímala drtivý podíl na trhu. Od roku 2019 však pod vlivem neustálých opatření Spojených států Huawei rychle ztratila svou drtivou převahu v podílu na trhu, zatímco společnosti Ericsson a Nokia začaly překvapivě tento trend obracet.[133]

4.3 Huawei jako nástroj politického vyjednání

Ještě pár měsíců před oficiálním zákazem společnosti Huawei se spekulovalo o potenciální obchodní dohodě s Čínou. V únoru americký ministr zemědělství Sonny Perdue uvedl, že čínští představitelé se zavázali nakoupit od Spojených států 10 milionů tun sóji. Perdue popisuje, že obchodní jednání Spojených států s Čínou zřejmě fungují a závazek k nákupům by označil za „projev dobré vůle ze strany Číňanů".[134] Podle deníku *Bloomberg* Čína zvažovala Trumpovou žádost o přesunutí některých čínských tarifů z klíčových zemědělských produktů na jiné produkty, aby mohla Trumpova administrativa případnou obchodní dohodu prodat jako výhru pro zemědělce před volbami v roce 2020.[135] Dle Johna Boltona byla otázka společnosti Huawei

[132] Tom Wheeler, „5G in Five (Not So) Easy Pieces." Brookings Institution, 9.července 2019, https://www.brookings.edu/articles/5g-in-five-not-so-easy-pieces/

[133] Daniel Gonzalez, Julia Brackup, Spencer Pfeifer, a Timothy M. Bonds, Securing 5G: A Way Forward in the U.S. and China Security Competition. Santa Monica, CA: *RAND Corporation*, 2022. https://www.rand.org/pubs/research_reports/RRA435-4.html.

[134] Ryan McCrimmon, „China Pledges Big Soybean Buy - Politico." Politico, February 1, 2019. https://www.politico.com/newsletters/morning-agriculture/2019/02/01/china-pledges-big-soybean-buy-498235.

[135] Bloomberg News, „China Considers U.S. Request to Shift Tariffs on Farm Goods." *Bloomberg News*, 15.dubna 2019. https://www.bloomberg.com/news/articles/2019-04-15/china-said-to-weigh-u-s-request-to-shift-tariffs-on-farm-goods.

klíčovou částí obchodních diskusí mezi prezidentem Trumpem a čínským prezidentem Si Ťin-pchingem.[136]

Uprostřed těchto jednání přišlo náhlé oznámení prezidenta Trumpa na *Twitteru* (později oficiálně potvrzené), že Spojené státy 10. května 2019 zvýší cla na dovoz z Číny z 10 % na 25 % v hodnotě 200 miliard dolarů.[137] Hned pár dní potom se Trumpova administrativa rozhodla zakázat obchodování se společností Huawei. Jak můžeme zpozorovat, kvůli neúspěšné dohodě Trump se rozhodl potrestat čínského „národního šampiona" v rámci obchodní války. Právě krátce poté, co prezident Trump prohlásil čínskou telekomunikační společnost za „velmi nebezpečnou" hrozbu pro americkou národní bezpečnost, uvedl, že by mohl zahrnout otázku Huawei do širší obchodní dohody mezi USA a Čínou.[138] Podobné prohlášení už uvedl v roce 2018, když byl dotázán, zda by byl ochoten propustit finanční ředitelku společnosti Huawei Meng výměnou za lepší obchodní dohodu. Podle Denise Wildera, bývalého vedoucího oddělení analýzy Číny v CIA, Trump jasně naznačil Číně, že jeho přístup k nim je spíše založen na obchodních transakcích, než aby řídil širšími ideologickými a strategickými principy.[139]

Bolton považuje Trumpova rozhodnutí týkajících se společnosti Huawei motivovaná především snahou o znovuzvolení než národními zájmy.[140] Během Trumpova zákazu již obě hlavní politické strany v USA, Demokratická strana i Republikánská strana, zmobilizovaly síly pro prezidentské volby v roce 2020. Trump potřeboval být rozhodný ve svém přístupu k Číně, aby si udržel své voliče – buď splnit sliby o výhodné obchodním dohodě pro USA, nebo zaujmout tvrdý postoj vůči Číně bez politických ústupků. Trump se obával, že pokud by podepsal

[136] John Bolton, *The Room Where It Happened*, 128.
[137] Spencer Kimball, „Trump Says Tariffs on $200 Billion of Chinese Goods Will Increase to 25%, Blames Slow Progress in Trade Talks." *CNBC*, May 5, 2019. https://www.cnbc.com/2019/05/05/trump-says-tariffs-on-200-billion-of-chinese-goods-will-increase-to-25percent-on-friday.html.
[138] Jana Lipská, „Podle Trumpa by Mohla Být Společnost Huawei Součástí Obchodní Dohody, Firmu Ale Označuje Za Nebezpečnou." *Seznam Zprávy*, 24.května 2019,
[139] Demetri Sevastopulo a Tom Mitchell. „Trump's Huawei Shift Angers US Security Hawks." Trump's Huawei Shift angers US security hawks, June 30, 2019. https://www.ft.com/content/c884d092-9b37-11e9-b8ce-8b459ed04726.
[140] John Bolton, *The Room Where It Happened*, 201.

obchodní dohodu s Čínou, která by byla vnímána jako slabá nebo nedostatečná, čelil by kritice ze strany demokratů.[141]

Během G20 summitu Trump čínskému prezidentovi řekl, že zvýšený nákup zemědělských produktů od amerických zemědělců z čínské strany by mohl zvýšit jeho šance na znovuzvolení. Jednání se zaměřovala právě na zvýšení objemu čínských nákupů amerických zemědělských produktů v tzv. nerozhodných státech (*swing states*), jako jsou Ohio, Iowa a Wisconsin. Právě tyto státy byly klíčové v prezidentských volbách v roce 2016, kde získal Donald Trump důležitou podporu voličů.[142] Dále to byli obyvatelé amerických venkovských oblastí, kteří přišli k volbám v dostatečném počtu, aby pomohli zajistit rozhodující vítězství ve těchto státech.[143] Podle ekonoma Paula Krugmana mají v americkém volebním systému „farmáři nepřiměřený politický vliv".[144] V letech 2013 až 2016 došlo v USA k markantnímu poklesu čistého příjmu zemědělských podniků o polovinu, což představuje největší tříleté snížení od Velké hospodářské krize. Vzhledem k této obtížné ekonomické situaci se vývoz zemědělských produktů do Číny stal klíčovým prvkem pro udržení ekonomické stability amerických farem a venkovských oblastí.[145] Farmáři a venkovští voliči mohli tedy zase sehrát v Trumpově znovuzvolení zásadní roli, a proto bylo nezbytné zajistit jejich spokojenost.

Nicméně celní válka Trumpovy administrativy proti Číně již poškodila jeho politickou podporu ze strany venkovských voličů. V polovině volebního období roku 2018 zaznamenali demokraté největší podíl hlasů ve venkovských volebních obvodech ve srovnání s volbami v roce 2016. Přestože Trumpova administrativa nabídla 28 miliard dolarů finanční podpory zemědělcům,

---

[141] Mark Lander a Ana Swanson. „Trump Sees a China Trade Deal through a New Prism: The 2020 Election." The New York Times, 11.května 2019. https://www.nytimes.com/2019/05/10/us/politics/trump-china-trade-2020-election.html.

[142] Pak Nung Wong, *Techno-Geopolitics: U.S.-China Tech War and the Practice of Digital Statecraft*, 2.

[143] Dan Balz, „Rural America lifted Trump to the Presidency. Support is strong, but not monolithic. " *Washigton Post* , 17.června 2017. https://www.washingtonpost.com/politics/rural-america-lifted-trump-to-the-presidency-support-is-strong-but-not-monolithic/2017/06/16/df4f9156-4ac9-11e7-9669-250d0b15f83b_story.html.

[144] Paul Krugman, „The Defrauding of America's Farmers." *The Palm Beach Post*, 2.září 2019, https://eu.palmbeachpost.com/story/opinion/columns/more-voices/2019/09/02/paul-krugman-defrauding-of-americas-farmers/3995180007/.

[145] Zhang Hongzhou,. „The U.S.-China Trade War: Is Food China's Most Powerful Weapon?" *Asia Policy* 15, č. 3 (2020): 65. https://www.jstor.org/stable/27023923.

výsledky voleb v polovině volebního období roku 2018 ukázaly, že zemědělci nebyli spokojeni. Proto Trump věděl, že je potřeba znovu získat ztracený americký podíl na čínském trhu.[146] A právě společnost Huawei, která byla nazývaná „národním šampionem Číny“ mohla pomoci přimět Peking koupit zemědělské produkty.

Senátoři Marco Rubio (republikán) a Mark Warner (demokrat), oba členové Výboru pro zpravodajské služby, poslali dopis americkému obchodnímu zmocněnci Robertu Lighthizerovi a ministru zahraničí Mikeu Pompeovi, v němž varovali před použitím Huawei jako vyjednávacího nástroje. V dopise americkému obchodnímu zmocněnci a ministru zahraničí senátoři Rubio a Warner uvedli, že Evropané mají obavy, že USA by mohly zmírnit postoj k Huawei, aby získali výhody v obchodních jednáních, jako tomu bylo v minulosti s firmou ZTE. Údajně byl potom Trump nespokojen, že se zákonodárci vměšují do jeho jednání.[147] Senátoři se proto rozhodli navrhnout zákon, který by zakázal odstranění Huawei z černé listiny Ministerstva obchodu bez souhlasu Kongresu a zabránil tak prezidentovi Trumpovi používat Huawei jako nástroj k vyjednání. [148]

[146]Ibid.,66.

[147] David Shepardson, „ U.S. senators urge Trump not to use Huawei as bargaining chip in trade talks‘‘, *Reuters,* 13.července 2019, https://www.reuters.com/article/idUSKCN1TE2E0/ (staženo 23.prosince 2023)

[148] Hadi Chapardar, William X. Wei, a Houssam Chamseddine „ Huawei in Canada: Doing Business in the Midst of Game of Thrones“ in in *Huawei Goes Global: Volume II: Regional, Geopolitical Perspectives and Crisis Management,* ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann, (London: Palgrave Macmillan, 2020), 132.

Závěr

V bakalářské práci jsem se zabývala analýzou politiky bývalého amerického prezidenta Donalda Trumpa vůči čínské společnosti Huawei, s důrazem na roli kybernetické bezpečnosti. Cílem práce bylo určit faktory, které přispěly k rozhodnutí Trumpovy administrativy bojkovat společnost Huawei. Práce odhalila, že administrativa Donalda Trumpa měla racionální důvody považovat Huawei za kybernetickou hrozbu, což bylo podloženo četnými čínskými kybernetickými aktivitami vůči USA. Jak bylo ukázáno v této práci, Huawei představovala národní bezpečnostní riziko pro Spojené státy již před Trumpovou administrativou kvůli svým vazbám na čínskou armádou. Nicméně výzkum také ukázal, že některé kroky Trumpovy administrativy vůči Huawei nebyly motivovány výhradně obavami o kybernetickou bezpečnost. Zdá se, že byly součástí širší strategie, zaměřené na zpomalení technologického pokroku Číny. Přesto je důležité si uvědomit, že úsilí o technologické vedení je úzce spjato s potřebou silné kybernetické bezpečnosti, a tedy zabezpečení nové 5G sítě je důležité pro omezení celkové průmyslové špionáže.

Trumpův postoj k Huawei ale naznačuje, že kybernetická bezpečnost ani technologické vedení nebyly hlavním faktorem v jeho rozhodnutí, ale především chtěl použít Huawei jako páku v obchodních jednáních s Čínou. Propojení obchodní politiky s kybernetickou bezpečností pod Trumpovou administrativou vedlo k nejasnostem při formování kybernetické politiky v rámci 5G a nepřesvědčilo tak všechny americké spojence k hromadnému bojkotu společnosti. Analýza politiky Donalda Trumpa vůči Huawei jasně ukazuje, že je nezbytné mít pevně promyšlenou strategii v kybernetické bezpečnosti. Přestože se Trump jevil jako nekonvenční a nezávislý aktér, stejně jako každý demokratický politický činitel, byl omezen domácími faktory. Je patrné, že americký prezident může být omezen Kongresem v otázkách zahraniční politiky a Kongres funguje tedy jako kontrolní orgán výkonné moci.

Během prezidentské kandidatury v roce 2024 by měli Trumpovi voliči pečlivě zvážit, zda přistupuje k otázkám národní bezpečnosti s odpovídající vážností, jak často tvrdí ve svých projevech a kampaních. Budoucí výzkum by mohl sledovat vývoj Bidenovy politiky vůči Huawei a analyzovat kontinuitu či změny v přístupu k problematice kybernetické bezpečnosti a politice vůči této společnosti.

Summary

In my bachelor's thesis, I analyzed the policy of former US President Donald Trump towards the Chinese company Huawei, with a focus on cybersecurity. The aim was to determine the factors contributing to the Trump administration's decision to boycott Huawei. The research revealed that the administration had valid reasons to consider Huawei a cybersecurity threat, supported by numerous Chinese cyber activities targeting the USA. It was also found that Huawei posed a national security risk to the United States due to its ties with the Chinese military even before the Trump administration.

However, the study also showed that some of the Trump administration's actions against Huawei were not solely motivated by cybersecurity concerns. They seemed to be part of a broader strategy aimed at slowing down China's technological progress. Nonetheless, it's important to recognize that efforts to lead in technology are closely linked to the need for strong cybersecurity, making securing the new 5G network crucial for limiting industrial espionage.

Trump's often-changing stance on Huawei suggests that cybersecurity or technological leadership weren't the primary factors in his decisions, but rather using Huawei as leverage in trade negotiations with China. This intertwining of trade policy with cybersecurity under the Trump administration led to ambiguities and failed to convince all American allies to collectively boycott the company.

The analysis of Trump's policy towards Huawei clearly demonstrates the necessity of having a stable and well-thought-out strategy in cybersecurity. Despite Trump's unconventional and independent image, like any democratic political figure, he was constrained by domestic factors. It's evident that the US president can be restricted by Congress in foreign policy matters, with Congress serving as a sort of oversight body for the executive branch.

Použité zdroje

Knihy

Alden, Chris a Amnon Aran. *Foreign Policy Analysis: New Approaches.* London: Routledge, 2017.

Allison, Graham. *Destiny for War – Can America and China Escape the Thucydides's Trap?*

Beach, Derek a Rasmus Brun Pedersen, *Process-Tracing Methods: Foundations and Guidelines*, Ann Arbor : University of Michigan Press, 2019.

Bolton, John. *The Room Where It Happened.* New York City: Simon & Schuster LLC, 2020. Boston: Houghton Mifflin Harcourt, 2017.

Fiřtová, Magdalena, Jan Hornát a Jana Sehnálková. 201*7. Prezidentství Baracka Obamy: naplněné vize?* Praha: Karolinum.

Fritz, Jason R. *China's Cyber Warfare: The Evolution of Strategic Doctrin*e. Lanham, MD: Lexington Books, 2017.

Choucri, Nazli a David Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma* . Cambridge, MA: MIT Press, 2018.

Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company, 2001.

Morin, Jean-Frédéric, a Jonathan Paquin. *Foreign Policy Analysis: A Toolbox.* London: Palgrave Macmillan, 2018.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* New York: Public Affairs, 2016.

Sørensen, Georg, Jørgen Møller, a Robert H. Jackson. *Introduction to International Relations: Theories and Approaches.* Oxford: Oxford University Press, 2022.

Warren, Aiden a Adam Bartley, *US Foreign Policy and China: The Bush, Obama, Trump Administrations*. Edinburgh: Edinburgh University Press, 2020
Wong, Pak Nung. *Techno-Geopolitics: U.S.-China Tech War and the Practice of Digital Statecraft*. London: Routledge, 2021.

Zhang, Wenxian, Ilan Alon a Christoph Lattemann, ed. Huawei Goes Global: Volume I: Made in China for the World. London: Palgrave Macmillan, 2020.

Primární zdroje

Congress. „NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2020'', 20.prosince 2019 , https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf

Čínská lidová republika, Státní rada. „Made in China 2025." 19. května 2015. https://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.html

Office of Public Affairs. Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors Systems to Steal Sensitive Military Information." 23.května 2016. https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

Office of the United States Trade Representative. „China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation." https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

The White House, „National Cyber Strategy of the United States America ", září 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (staženo 7.prosince 2023).

Trump, Donald J. „Executive Order on Securing the Information and Communications Technology and Services Supply Chain." White House, 15.května 2019. https://trumpwhitehouse.archives.gov/presidential- actions/executive-order-securing-information-communications-technology-services-supply-chain/

United States of America. „National Security Strategy of the United States of America", prosinec 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (staženo 13.prosince 2023).

Rozhovory a projevy

Pompeo, Mike. Interview vedla Maria Bartiromo, Mornings With Maria, *Fox Business Network*, 6.února 2019. https://2017-2021.state.gov/interview-with-maria-bartiromo-of-mornings-with-maria-on-fox-business-network-2/https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors- systems-steal-sensitive

Trump, Donald „ Remarks by President Trump on United States 5G Deployment", 12.dubna 2019, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-united-states-5g- deployment/ (přístup 19. prosince 2023)

Hudson Institute. "Vice President Mike's Remarks on the Administration's Policy Towards China." 4.října 2018. https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towardschina102018.

Kapitoly v knize

Blanchard, Jean-Marc F. „Helping Hands for Huawei: Dialing into China's Technology Policy to Understand Its Contemporary Support for Huawei" in *Huawei Goes Global: Volume I: Made in China for the World*, eds. Wenxian Zhang, Ilan Alon, Christoph Lattemann. London: Palgrave Macmillan, 2020.

Cottam, Martha. "Foreign Policy Decision Making in the Trump Administration," in *The Trump Doctrine and the Emerging International System*, ed. Stanley A. Renshon, Peter Suedfeld. London: Palgrave Macmillan, 2021

Chapardar, Hadi, William X. Wei, a Houssam Chamseddine „ Huawei in Canada: Doing Business in the Midst of Game of Thrones" in in *Huawei Goes Global: Volume II: Regional, Geopolitical Perspectives and Crisis Management*, ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann, London: Palgrave Macmillan, 2020

Jervis, Robert „President Trump and International relations theory “, in *Chaos in the Liberal Order: The Trump Presidency and International Politics in the Twenty-First Century*, ed. Robert Jervis, Francis J. Gavin, Joshua Rovner a Diana N. Labrosse. New York: Bloomsbury Publishing, 2013.

Kirste, Laura a Dirk Holtbrügge. „Huawei at Bay? A View on Dependency Theory in the Information Age” in *Huawei Goes Global: Volume I: Made in China for the World,* ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann. London: Palgrave Macmillan, 2020.

Kjellman, Anders, Xiaohua Yang, Xiaobo Wu, and Sun-Young Park. „*Huawei's Expansion and Nokia's Retreat: What Lessons Can We Learn?*” in *Huawei Goes Global: Volume I: Made in China for the World*, ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann. London: Palgrave Macmillan, 2020.

Lourie, Tom. „The Decision Calculus of Donald Trump”, in *How Do Leaders Make Decisions?*, ed. Alex Mintz A Dmitry Adamsky. Leeds: Emerald Publishing Limited, 2019.

Rezková, Alice. „ Čínská karta v amerických prezidentských volbách“ v *America First Příčiny a kontext volebního vítězství Donalda Trumpa*, ed, Jan Hornát a Lucie Kýrová . Praha: Karolinum, 2020.

Schortgen, Francis. “Weaponizing Globalization: Chinese High-Tech in the Crosshairs” in *Huawei Goes Global: Volume I: Made in China for the World,* ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann. London: Palgrave Macmillan, 2020.

Tsang, Denise a David Luigi Fuschi, „A Strategic Assessment of Huawei into the Fast Future“ in *Huawei Goes Global: Volume I: Made in China for the World*, ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann, London: Palgrave Macmillan, 2020

Valeriano, Brandon. "China and the Technology Gap: Chinese Strategic Behavior in Cyberspace" in *Cyber Strategy: The Evolving Character of Power and Coercion*, ed. Brandon Valeriano, Benjamin Jensen a Ryan C. Maness. Oxford: Oxford University, 2019.

Ze Yu, Shirley. „All Under Huawei: China's New Vision for a Tech Sinica" in *Huawei Goes Global: Volume I: Made in China for the World,* ed. Wenxian Zhang, Ilan Alon, a Christoph Lattemann. London: Palgrave Macmillan, 2020.

Elektronické publikace

Bateman, Jon. *U.S.-China Technological "Decoupling": A Strategy and Policy Framework.* Washington D.C: Carnegie Endowment for International Peace, 2022. https://carnegieendowment.org/files/Bateman_US- China_Decoupling_final.pdf

Branstetter, Lee, a Li Guangwe. „The Actual Effect of China's 'Made in China 2025' Initiative May Have Been Overestimated." *CEPR*, 11. srpna 2023. https://cepr.org/voxeu/columns/actual-effect-chinas-made-china-2025- initiative-may-have-been-overestimated

Deloitte. „ United States expands global lead in mobile broadband'', září 2014, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt- mobile-index-09262014.pdf (staženo 12. prosince 2023).

Department of Homeland Security. „5G Impacts on Cybersecurity." 28. září 2023. https://www.dhs.gov/sites/default/files/2023 09/23_0906_oia_01_5G_Security_508_Compliant.pdf.

Gallagher, Jill C. „U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests. " Washington D.C: Congressional Research Service, 5. ledna 2022. https://crsreports.congress.gov/product/pdf/R/R47012/2 (staženo 2. prosince 2023).

Gonzales, Daniel, Julia Brackup, Spencer Pfeifer a Timothy M. Bonds. „ Securing 5G: A Way Forward in the U.S. and China Security Competition." Santa Monica, CA: RAND Corporation, 2022. https://www.rand.org/pubs/research_reports/RRA435-4.html

Jensen, Benjamin. „How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy." *CSIS*, 19.října 2023. https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber- espionage-undermine-american-economy

Joint Chiefs of Staff, *Joint Publication 3-12 (R): Cyberspace Operations*. Washington D.C., 2018. https://irp.fas.org/doddir/dod/jp3_12r.pdf (staženo 11.prosince.2023).

Kidwell, Deborah. „Cyber Espionage for the Chinese Government." *Office of Special Investigations,* 17.září 2020. https://www.osi.af.mil/News/Features/Display/Article/2350807/cyber-espionage-for-the-chinese- government/

Lee, Nicol. „Navigating the U.S.-China 5G Competition", *Brookings Institution*, https://www.brookings.edu/articles/navigating-the-us-china-5g-competition/.

Lobell, Steven. „Structural Realism/Offensive and Defensive Realism. Oxford Research Encyclopedia of International Studies". 22.prosince 2017. https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore- 9780190846626-e-304 (staženo 27.listopadu 2023).

Medeiros, Evan S., Roger Cliff, Keith Crane a James C. Mulvenon. „ A New Direction for China's Defense Industry. " *RAND Corporation*, 2005, https://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG334.pdf

Mello, Peter A., and Frank Ostermann, eds. *Routledge Handbook of Foreign Policy Analysis Methods, London : Routledge*, 2022, https://doi.org/10.4324/9781003139850.

National Counterintelligence and Security Center. „Foreign Economic Espionage in Cyberspace." 2018. https://www.dni.gov/files/NCSC/documents/news/
NIS Cooperation Group. „EU coordinated risk assessment of the cybersecurity of 5G networks." 9. října 2019. https://www.politico.eu/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf

Smith, Nicholas R. „Using Process-Tracing to Drive Foreign Policy Analysis: Strengths and Weaknesses in the Context of Analyzing the Foreign Policies of the EU and Russia in the Context of the Ukraine Crisis." In Sage Research Methods Cases Part 2. London: Sage Publications Ltd., 2024. https://doi.org/10.4135/9781526462404.

Wheeler, Tom „5G in Five (Not So) Easy Pieces." Brookings Institution, 9.července 2019, https://www.brookings.edu/articles/5g-in-five-not-so-easy-pieces/

World Economic Forum. „The Impact of 5G: Creating New Value across Industries and Society". *World Economic Forum*, leden 2020. https://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf

Yee, William Yuen. „With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?: New Perspectives on Asia." *CSIS*, 10.prosince 2020. https://www.csis.org/blogs/new-perspectives-asia/us- restrictions-huawei-and-zte-where-will-rural-america-turn

Odborné články

Bowling, C. J., Fisk, J. M., & Morris, J. „Seeking Patterns in Chaos: Transactional Federalism in the Trump Administration's Response to the COVID-19 Pandemic", *The American Review of Public Administration,* 50(6-7), 512-518, (16.června 2020), https://doi.org/10.1177/0275074020941686 (staženo 4.dubna 2024)

Evans, Paul „Techno-nationalism in China–US Relations: Implications for Universities." *East Asian Policy* 12, č. 2 (2020): 85.

Huang, Keman, Stuart Madnick, Fang Zhang a Michael Siegel. „Varieties of public–private co-governance on cybersecurity within the digital trade: implications from Huawei's 5G.''*Journal of Chinese Governance* 7, č. 1 (2022): 87. https://www.tandfonline.com/doi/full/10.1080/23812346.2021.192323

Peng, Xinyan. „The Essence and Impact of US-China Technology Competition", A*dvances in Social Science, Education and Humanities Research*, 11.července 2023, 754–59. https://doi.org/10.2991/978-2-38476-062-6_97

Wang, Liying. „China's Huawei in the US-China Trade War in the Communications Sector Game." In *Proceedings of the 2022 2nd International Conference on Enterprise Management and Economic Development (ICEMED 2022), Advances in Economics, Business and Management Research, volume 219* , Atlantis Press, 2022. doi:10.2991/aebmr.k.220603.078.

Xu, Manshu a Chuanying Lu. „ China–U.S. Cyber-Crisis Management.*" China International Strategy Review* 3, 105 (28.června 2021). https://link.springer.com/article/10.1007/s42533-021-00079-7

Zhang Hongzhou,. „The U.S.-China Trade War: Is Food China's Most Powerful Weapon?" *Asia Policy* 15, č. 3 (2020): 59–86. https://www.jstor.org/stable/27023923.

Diplomové práce a disertační práce

Mazák, Jaromír. „Občanská společnost jako aktér politického procesu." Disertační práce,Univerzita Karlova, 2019.

Pastorková, Sabrina. „Foreign Policy of Trump's Administration: Withdrawal from the Paris Accord through the Lens of Two-Level Game Theory." Diplomová práce, Univerzita Karlova, 2019.

Webové stránky

ARCEP. „5G et empreinte environnementale des réseaux: de nouveaux travaux de l'Arcep pour éclairer le débat et identifier des leviers d'action." https://www.arcep.fr/actualites/actualites-et- communiques/detail/n/environnement-140122.html

Council on Foreign Relations. „Cyber Operation Tracker." https://www.cfr.org/cyber-operations/

Huawei. „ Who owns Huawei?'', https://www.huawei.com/ke/facts/question-answer/who-owns-huawei.

Ministerstvo vnitra České republiky. „Ochrana kritické infrastruktury." https://www.mvcr.cz/chh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx

Národní úřad pro kybernetickou a informační bezpečnost. „Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice." , 7.února 2022 https://nukib.gov.cz/cs/infoservis/doporuceni/1801- doporuceni-pro-hodnoceni-duveryhodnosti-dodavatelu-technologii-do-5g-siti-v-ceske-republice/

Národní úřad pro kybernetickou a informační bezpečnost. „Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou“, 17.prosince 2018, https://nukib.gov.cz/cs/infoservis/aktuality/1303-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/ (staženo 19. listopadu 2023).

Grafy

Center for Strategic and International Studies, „ Survey of Chinese Espionage in the United States Since 2000‘‘ březen 2023, https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000, (přístup 23.prosince 2023).

Novinové články

Arthur, Charles. „China’s Huawei and ZTE Pose National Security Threat, Says US Committee”. *The Guardian. 8*.října 2012. https://www.theguardian.com/technology/2012/oct/08/china-huawei-zte-security-threat (staženo 19.listopadu 2023).

Balz, Dan. „Rural America Lifted Trump to the Presidency. Support is strong, but Not Monolithic. ” *Washigton Post,* 17.června 2017. https://www.washingtonpost.com/politics/rural-americalifted-trump-to-the-presidency-support-is-strong-but-not-monolithic/2017/06/16/df4f9156-4ac9-11e7-9669-250d0b15f83b_story.html.

Blatchford, Andy a Leah Nylen. „Trump’s Comments about Huawei Exec’s Arrest to Take Center Stage in Extradition Fight.” *POLITICO*, 15.června 2020, https://www.politico.com/news/2020/06/15/trump-china-trade- deal-huawei-executive-extradition-319642

Bloomberg News. „China Considers U.S. Request to Shift Tariffs on Farm Goods.” *Bloomberg News*, 15. května 2019.https://www.bloomberg.com/news/articles/2019-04-15/china-said-to-weigh-u-s-request-to-shift-tariffson-farm-goods

Briefing. „ Huawei Is at the Centre of Political Controversy.” *The Economist*, 27. dubna 2019. https://www.economist.com/briefing/2019/04/27/huawei-is-at-the-centre-of-political-controversy.
ČTK. „ “Přispěje k národní bezpečnosti." Babiš podepsal s americkým ministrem zahraničí deklaraci o 5G sítích.” *iROZHLAS*, 6.května 2020, https://www.irozhlas.cz/veda-technologie/technologie/andrej-babis-mike- pompeo-5g-mobilni-site-dodavatele-usa-cesko_2005062234_dok

Everett Rosenfeld. „US-China Agree to Not Conduct Cybertheft of Intellectual Property.” *CNBC*, 25.září 2015, https://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-propertywhite-house.html.

Geller, Eric. „Mueller’s Timeline: How the Russian Hacks Unfolded - Politico.” *Politico* , 13.června 2018. https://www.politico.com/story/2018/07/13/mueller-russia-hacks-timeline-686521.

Gol, Joe. „ Esper to Allies: Picking Huawei Risks Intel and Security Ties with the US.” *Defense News*, 15.února 2020.https://www.defensenews.com/congress/2020/02/15/esper-huawei-5g-could-risk-us-information-and-security-ties/ (staženo 7.prosince 2023).

Greenberg, Andy. „Trump’s Worst, Most Bizarre Statements about ‘The Cyber.’ *Wired,* 18.ledna 2021 https://www.wired.com/story/trump-cyber-worst-quotes-statements-hackers-ukraine-russia/.(staženo 23.12.2023).

Hille, Kathrin. „Huawei’s Emergence from Shadows Backfires.” *Financial Times*, 8.října 2012. https://www.ft.com/content/50ad88c2-112b-11e2-a637-00144feabdc0.

Holcová, Pavla. „Co je špatně (s) Huawei?!” *investigace.cz*, 29.října 2019. https://www.investigace.cz/co-je-spatne-shuawei/.

Kadiri, Ghalia a Joan Tilouine. „A Addis-Abeba, Le Siège de l'Union Africaine espionné par Pékin.” *Le Monde*, 26. ledna 2018. https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-unionafricaine-espionne-par-les-chinois_5247521_3212.html. (staženo 17.dubna 2024)

Kang, Cecilia a David E. Sanger. „Huawei Is a Target as Trump Moves to Ban Foreign Telecom Gear." *The New York Times*, 15.května 2019. https://www.nytimes.com/2019/05/15/business/huawei-ban-trump.html

Kimball, Spencer. „Trump Says Tariffs on $200 Billion of Chinese Goods Will Increase to 25%, Blames Slow Progress in Trade Talks." CNBC, 5.května 2019. https://www.cnbc.com/2019/05/05/trump-says-tariffs-on-200-billion-of-chinesegoods-will-increase-to-25percent-on-friday.html.

Kuo, Lily. „Huawei Sues Us over Government Ban on Its Products." *The Guardian*, 7.března 2019. https://www.theguardian.com/world/2019/mar/07/huawei-sues-us-over-government-ban-on-its-products

Lander, Mark a Ana Swanson. „Trump Sees a China Trade Deal through a New Prism: The 2020 Election." The New York Times, 11.května 2019. https://www.nytimes.com/2019/05/10/us/politics/trump-china-trade2020-election.html

Link, Jordan. „How Huawei could survive Trump", *Washington Post* , 10.června 2019. https://www.washingtonpost.com/politics/2019/06/10/what-do-we-know-about-huaweis-africa-presence/, (staženo 27.listopadu 2023).

Lipská, Jana „Podle Trumpa by mohla být společnost Huawei součástí obchodní dohody, firmu ale označuje za nebezpečnou." *Seznam Zprávy*, 24.května 2019, https://www.seznamzpravy.cz/clanek/podle-trumpa-by-mohla-bytspolecnost-huawei-soucasti-obchodni-dohody-firmu-ale-oznacuje-za-nebezpecnou-72593. (staženo 17. dubna 2024).

Mackinnon, Amy. „For Africa, Chinese-Built Internet Is Better than No internet at All, " *Foreign Policy,* 19. května 2019. https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is- better-than-no-internet-at-all/(staženo 27.listopadu 2023).

Marks, Joseph. „ The Cybersecurity 202: Trump's ban on U.S. companies supplying Huawei will not make the country safer experts say", *The Washigton Pos*t, 4.června 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-

202/2019/06/04/the-cybersecurity- 202-trump-s-ban-on-u-s-companies-supplying-huawei-will-not-make-the-country-safer-experts- say/5cf5c40ba7a0a46b92a3ff86/(staženo 17.prosince 2023).

Nakashima, Ellen a Josh Dawsey, „Trump Administration Cracks down on Giant Chinese Tech Firm, Escalating Clash with Beijing", *The Washington Post*, 16. května 2019, https://www.washingtonpost.com/world/national-security/trump-signs-order-to-protect-us-networks-from-foreign-espionage-a-move-that-appears-to-target- china/2019/05/15/d982ec50-7727-11e9-bd25-c989555e7766_story.html (staženo 26.listopadu 2023)

Rappeport, Alan a Ana Swanson. „Trump Renews Trade War as China Talks End without a Deal, ''*The New York Times,* 10.května, 2019, https://www.nytimes.com/2019/05/10/us/politics/trump-china-trade.html.

Salinas, Sara. „Six Top US Intelligence Chiefs Caution against Buying Huawei Phones." *CNBC*, 15.února 2018. https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html

Sanger, David E. a Nicole Perlroth, „N.S.A. Breached Chinese Servers Seen as Security Threat." The New York Times, 22.března 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html. (staženo 7.prosince 2023)

Sevastopulo, Demetri a Tom Mitchell. „Trump's Huawei Shift Angers US Security Hawks." *Financial Times,* 30.června 2019. https://www.ft.com/content/c884d092-9b37-11e9-b8ce8b459ed04726

Shepardson, David „U.S. senators urge Trump not to use Huawei as bargaining chip in trade talks'', *Reuters,* 13.července 2019, https://www.reuters.com/article/idUSKCN1TE2E0/ (staženo 23.prosince 2023)

Shepardson, David, a Karen Freifeld. "China's Huawei, 70 Affiliates Placed on U.S. Trade Blacklist." *Reuters*, 16.května 2019. https://www.reuters.com/article/us-usa-china-huaweitech-idUSKCN1SL2W4/

Shu, Catherine. „New Defense Bill Bans the U.S. Government from Using Huawei and ZTE Tech." *TechCrunch*, 15. srpna 2018. https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-using-huawei-and-zte-tech/
Schmidt, Michael S, Keith Bradsher a Christine Hauser. „U.S. Panel cites risks in Chinese equipment." *The New York Times*, 8.října 2012. https://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html.

Staudenmaier, Rebecca. „German Minister Warns of 5G Delays If Huawei Is Left out." *Deutsche Welle*, 18.ledna 2020. https://www.dw.com/en/germanys-seehofer-warns-of-5g-delays-if-huawei-is-excluded/a- 52050565

Stracqualursi, Veronica, Kevin Liptak, a Jennifer Hansler. „Trump Downplays Massive Cyber Hack on Government after Pompeo Links Attack to Russia" , CNN, 19.prosince 2020, https://edition.cnn.com/2020/12/19/politics/pompeo-usgovernment-hack-russia/index.html.
Swanson, Anna. U.S. Delivers Another Blow to Huawei with New Tech Restrictions." *The New York Times,* 15.května 2020, https://www.nytimes.com/2020/05/15/business/economy/commerce-department-huawei.html.

Tan, Huileng. "Trump Faces Pushback after Saying He May Intervene in Arrest of Huawei Executive." *CNBC*, 13. prosince 2018. https://www.cnbc.com/2018/12/13/huawei-cfo-arrest-pushback-against-trump-who-says-he- may-intervene.html

Tang, Frank a Ji Siqi. „Starved of Chips, China Faces 'unprecedented' Pressure to Become No 1 Economy." *South China Morning Pos*t, 13.dubna 2023. https://www.scmp.com/economy/china-economy/article/3209385/tech-war-starved-semiconductors-chinas-bid-topple-us-no-1-economy-faces-unprecedented-pressure.

Tao, Li. „Huawei Executive Says Company Has Little to Do with Beijing's 2025 Plan." *South China Morning Post*, 8. listopadu 2018. https://www.scmp.com/tech/enterprises/article/2172158/huaweis-ken-hu-says-company- has-little-do-beijings-ambitious-2025 (staženo 23.prosince 2023)

Uznaska, Paulina. „Will Poland Be an Anti-Huawei Force in the EU?" *The Diplomat*, 27.srpna 2020. https://thediplomat.com/2020/08/will-poland-be-an-anti-huawei-force-in-the-eu/

Weisman, Steven R. “Sale of 3Com to Huawei Is Derailed by U.S. Security Concerns.” *The New York Times*, 21. února 2008. https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html

Yap, Chuin-Wei . „State Support Helped Fuel Huawei’s Global Rise” , *The Wall Street Journal,* 25.prosince, 2019, https://www.wsj.com/articles/state-sup- port-helped-fuel-huaweis-global-rise-11577280736 (staženo 27.listopadu 2023).