UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

Institut mezinárodních studií

Katedra severoamerických studií

Diplomová práce

2024 **Lucie Kenkušová**

UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

Institut mezinárodních studií

Katedra severoamerických studií

Komparace přístupu k problematice kybernetické bezpečnosti Spojených států amerických a Spojeného království

Diplomová práce

Autorka práce: Lucie Kenkušová

Studijní program: Mezinárodní teritoriální studia – severoamerická studia

Vedoucí práce: PhDr. Pavel Szobi, 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 15. 12. 2023 Lucie Kenkušová

Bibliografický záznam

KENKUŠOVÁ, Lucie. *Komparace přístupu k problematice kybernetické bezpečnosti Spojených států amerických a Spojeného království.* Praha, 2024. 98 s. Diplomová práce (Mgr.). Univerzita Karlova, Fakulta sociálních věd, Institut mezinárodních studií, Katedra severoamerických studií. Vedoucí diplomové práce PhDr. Pavel Szobi Ph.D.

Rozsah práce: 181 961

Abstrakt

Tato diplomová práce představuje komparaci strategií kybernetické bezpečnosti Spojených států amerických a Spojeného království. Čím vyspělejší společnost je, tím větší bývá její digitalizace a závislost na kyberprostoru. Vzhledem k této závislosti jsou státy mimořádně náchylné k interním či externím kybernetickým útokům a útokům na jejich informační systémy. Vytváří se tím zcela nová zranitelná místa, jak pro státy jako takové, tak pro celou společnost. Tato práce blíže představuje a komparuje mechanismy institucionálních reakcí obou států v případě kybernetického incidentu. Tyto mechanismy jsou přiblíženy jak na pozadí historického vývoje kybernetických strategií, tak i demonstrovány na vybraných kybernetických incidentech. Jak Spojené státy, tak Spojené království využívají jako hlavní mechanismus zvládání kybernetických hrozeb metodu cyber detterance, která byla použita i při zmíněných útocích. Práce si klade za cíl přiblížit účinnost této strategie a zasadit jí do kontextu strategie kybernetické bezpečnosti. Ukazuje se, že ač by přístup cyber detterance měl být nedílnou součástí strategie kybernetické bezpečnosti každého státu, bylo by vhodné věnovat zvýšenou pozornost i ostatním přístupům a rovněž přípravám i ofensivních kybernetických strategií.

Abstract

This thesis presents a comparison of the cybersecurity strategies of the United States and the United Kingdom. The more advanced a society is, the more it tends to be digitised and dependent the security of cyberspace. Due to this dependence, states are extremely vulnerable to internal or external cyber attacks and assaults on their information systems. This creates entirely new vulnerabilities, both for states as such and for society as a whole. This thesis presents and compares the institutional response mechanisms of both states in the event of a cyber incident. These mechanisms are approached against the backdrop of the historical development of cyber strategies as well as demonstrated through selected cyber incidents. Both the United States and the United Kingdom use the cyber deterrence method as their main mechanism for dealing with cyber threats, which was also used in the aforementioned attacks. This thesis aims to present the effectiveness of this strategy and place it in the context of cyber security strategy as a whole. It shows that although the cyber detterance approach should be an integral part of every state's cybersecurity strategy, it would be advisable to pay increased attention to other approaches as well as to the

preparation of offensive cyber strategies.

Klíčová slova

[kybernetická bezpečnost, kybernetické hrozby, kybernetické strategie, Spojené státy americké, Spojené království, cyber deterrance]

Keywords

[cyber security, cyber threats, cyber strategies, United States, United Kingdom, cyber deterrance]

Title/Název práce

Komparace přístupu k problematice kybernetické bezpečnosti Spojených států amerických a Spojeného království

Comparison of approaches to cybersecurity issues of the United States and the United Kingdom

Poděkování

Na tomto místě bych ráda poděkovala panu PhDr. Pavlovi Szobimu Ph.D. za odborné vedení, za jeho cenný čas a otevřený přístup při revidování práce.

Obsah

Úvod

V současné době, kdy se svět stále více posouvá do digitálního prostoru, se kybernetická bezpečnost stává klíčovou oblastí, která vyžaduje pozornost a detailní zkoumání. Tato diplomová práce se zaměřuje na analýzu a porovnání kybernetických strategií a reakcí na kybernetické incidenty ve Spojených státech amerických a ve Velké Británii. Obě tyto země se vyznačují vysokou mírou digitalizace a každý den čelí výzvám v oblasti kybernetické bezpečnosti.

Studium kybernetické bezpečnosti je zásadní z několika důvodů. Za prvé, kyberprostor se stává prostředím, kde se odehrává stále více našich každodenních aktivit, což zvyšuje riziko kybernetických útoků, které mohou mít závažné důsledky pro jednotlivce, firmy i vlády. Za druhé, kybernetické útoky jsou čím dál více sofistikovanější a jejich dopady jsou stále závažnější, což vyžaduje neustálé inovace a adaptaci v strategiích kybernetické bezpečnosti.

Spojené státy se svou technologickou vyspělostí a rolí globálního lídra nabízejí jedinečný pohled na strategie a výzvy v oblasti kybernetické bezpečnosti. Jejich přístup ke kybernetickým hrozbám, tvorbě politik a zavádění bezpečnostních opatření slouží jako zásadní případová studie pro pochopení širších důsledků kybernetické bezpečnosti. Podobně i přístup Velké Británie, který je formován jejím vlastním politickým, sociálním a technologickým kontextem, poskytuje cenné srovnání. Nabízí pohled na to, jak odlišné regulační prostředí, kulturní perspektivy a technologické rámce ovlivňují strategie kybernetické bezpečnosti.

Srovnáním těchto dvou zemí chce tato práce poukázat na význam kybernetické bezpečnosti v současném světě a zasadit se o to, aby se této kritické oblasti věnovala zvýšená pozornost. Snaží se pochopit, jak mohou různé strategie vést k různým výsledkům v boji proti kybernetickým hrozbám a jaké poučení si lze vzít z těchto dvou příkladných modelů, ať už co do reakce na konkrétní kybernetické incidenty anebo co do jejich institucionálního aparátu. Spojené státy americké a Spojené království, jakožto přední světové mocnosti, se významně podílejí na formování globálních standardů v oblasti kybernetické bezpečnosti a

jejich přístupy k této problematice mají vliv na celosvětovou bezpečnostní situaci.

Spojené státy a Velká Británie přijaly jako ústřední strategii v zabezpečení svého kyberprostoru přístup cyber detterance (odstrašování). Tato práce se na problematiku kybernetické bezpečnosti dívá rovněž optikou cyber detterance. Tento přístup slouží především jako preventivní opatření, které signalizuje schopnost a ochotu obou zemí odpovědět na kybernetické útoky, a tím odrazuje potenciální agresory. Cyber detterance nabízí širokou škálu reakcí, od diplomatických po kybernetické protiútoky, což umožňuje přiměřené odpovědi na různé úrovně hrozeb. Kromě toho napomáhá zavádění mezinárodních norem a standardů v kyberprostoru, čímž podporuje stabilnější a bezpečnější digitální prostředí. Tento přístup je účinný při zmírňování rizik závažných kybernetických útoků, neboť možnost silné odvetné reakce může státní i nestátní aktéry odradit od zahájení kybernetických operací s velkým dopadem.

Cílem této práce je poskytnout ucelený pohled na současný stav kybernetické bezpečnosti ve Spojených státech a ve Spojeném království a identifikovat klíčové faktory ovlivňující efektivitu jejich strategií v této oblasti. Autorka tímto způsobem chce přispět k diskusi o globálních trendech v oblasti kybernetické bezpečnosti. Limity své práce spatřuje v omezených zdrojích, týkající se této problematiky, detailní informace o kybernetických incidentech často nejsou veřejně dostupné. Práce se opírá především o národní strategie kybernetické bezpečnosti jak ze Spojených států, tak ze Spojeného království. Dalšími důležitým zdrojem je také ústřední zpráva pro členy amerického kongresu, zveřejněná v roce 2022, která představuje cyber deterrance jako jednu z hlavních strategií Spojených států v oblasti kybernetické bezpečnosti. Tato zpráva analyzuje strategii cyber deterrance ve vztahu ke kybernetickým útokům a rozebírá možnosti, které může Kongres využít při prosazování politiky cyber deterrance.

1. Definice pojmů a úvod do problematiky

1.1. Kyberprostor a kybernetická bezpečnost

Terminologie kyberprostoru se stále vyvíjí a v současnosti neexistuje jeho ustálená definice. Samotný pojem kyberprostoru se už od jeho stvoření v 80. letech 20. století úzce vázal k vizi nefyzického, virtuálního prostředí generovaného počítači.[1] V následujících letech, když začal být patrný rychlý a masivní nástup komunikačních technologií, začal být kyberprostor chápán jako součást informační sféry.[2] V současné době ministerstvo obrany Spojených států definuje kyberprostor jako globální doménu v rámci informačního prostředí sestávající ze vzájemně závislé sítě infrastruktur informačních technologií, zahrnující internet, telekomunikační sítě, počítačové systémy a vestavěné procesory a řadiče.[3]

Obecně lze říci, že operace, které se odehrávají v kyberprostoru, zahrnují tři dimenze informačního prostředí – poznávání, obsah a konektivitu. Poznávání se soustřeďuje na lidské vnímání, rozhodování a interakci v kyberprostoru. Jeho studium zahrnuje disciplíny, jako je neurobiologie, psychologie, filozofie a etika. V dnešní diskusi o národní bezpečnosti je poznávání pravděpodobně nejméně zdůrazňovaným prvkem kyberprostoru. Druhá dimenze, obsah se vztahuje k informacím, které jsou vytvářeny (nebo ničeny), přenášeny a ukládány v kyberprostoru. Může mít mnoho podob, z nichž drtivá většina v současnosti zahrnuje digitální obrazy přenášené elektronickými prostředky. Je to pravděpodobně nejvíce zdůrazňovaný prvek kyberprostoru s velkým zaměřením na softwarové programy, které mohou vytvářet nebo ničit data na mnoha úrovních. Konektivita představuje fyzické platformy a struktury, které usnadňují kognitivní a obsahovou dimenzi v kybernetickém prostoru. Je to nejviditelnější dimenze (např. osobní počítače, mobilní zařízení a mobilní věže), a tudíž pravděpodobně nejsnáze pochopitelná pro průměrného občana. Hranice mezi těmito dimenzemi nejsou rigidní, ale často se

[1] Bastl, Martin, Gruberová, Zuzana, Kyberprostor jako „pátá doména"?, *Vojenské rozhledy*, 2013, roč. 22 (54), č. 4, s. 10-21, ISSN 1210-3292, www.vojenskerozhledy.cz (staženo 3. 5. 2023).
[2] Alberts, D.- Garstka, J.- Stein, F. Network Centric Warfare. 2. vyd., Washington: CCRP, 2000, 284 s. ISBN 1-57906-019-6
[3] S. Deputy Secretary of Defense Gordon England, "The Definition of 'Cyberspace'," Memorandum for Secretaries of the Military Departments, Washington, DC, 12. 5. 2008, integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm (staženo 3. 5. 2023).

překrývají (např. sociální sítě).[4]

Vznik kyberprostoru, který je nyní označován za pátou válečnou doménu, vyvolal nové otázky, týkající se lidské odpovědnosti za operace v kyberprostoru a odpovědnosti za přímé ekonomické, sociální, kulturní, politické a technologické dopady této rychle se vyvíjející a nepředvídatelné domény, která je naprosto odlišná od ostatních oblastí, kde tradičně dochází ke konfliktům, jako jsou vzduch, vesmír, země a moře. S kyberprostorem se propojily téměř všechny aspekty lidské činnosti.[5]

Děje se tak rychlostí, jakou dosud nikdo nezažil. Kyberprostor, nová, umělá sféra, která zasahuje do reálného světa, se vyvinula v naprosto nové prostředí, ve kterém se stále učíme pohybovat. Je provázána s již existujícími doménami a podstatně ovlivňuje fungování světového politického a ekonomického systému. Spojené státy i Velká Británie označily terorismus a kybernetické útoky za dvě největší hrozby pro národní bezpečnost v jednadvacátém století.

Možnost volného přístupu a působení v kyberprostoru je považována za životně důležitý zájem pro suverenitu a prosperitu všech států. To dokládá například i fakt, že v době, kdy se federální rozpočet Spojených států určený na obranu státu výrazně snižuje, je financování související s kyberprostorem obecně na vzestupu. Kybernetická bezpečnost jako taková spočívá v umění zabránit neoprávněnému přístupu k sítím, zařízením a datům a zároveň v zachovávání důvěrnosti, integrity a přístupnosti informací. V dnešní době je v kyberprostoru operační prostor pro řadu klíčových odvětví jak pro stát, tak pro jednotlivce.

Ještě donedávna se termín národní bezpečnost při diskusích o kyberprostoru používal převážně pouze v rámci Spojených států. Rozšířené zavádění speciálních národních bezpečnostních strategií (NSS) v řadě zemí Organizace pro hospodářskou spolupráci a rozvoj (OECD) je relativně novým jevem, který je úzce spjatý s posunem strategického

[4] Caton, Jeffrey L., And J. Boone Bartholomees. "On The Theory Of Cyberspace." Volume I: Theory Of War And Strategy, Strategic Studies Institute, US Army War College, 2012, str. 325–44. JSTOR, Http://Www.Jstor.Org/Stable/Resrep12116.26 (staženo 5. 5. 2023).
[5] Bastl, Martin, Gruberová, Zuzana, Kyberprostor jako „pátá doména"?, *Vojenské rozhledy*, 2013, roč. 22 (54), č. 4, s. 10-21, ISSN 1210-3292, www.vojenskerozhledy.cz (staženo 3. 5. 2023).

myšlení od zaměření se pouze na několik specifických hrozeb spíše k myšlence zmírnění rizik obecně a snaze jim předejít. Podle Evropské agentury pro bezpečnost sítí a informací (ENISA) v současnosti neexistuje jednotná definice kybernetické bezpečnosti, kterou by sdílely státy na úrovni EU nebo obecně na mezinárodní úrovni. Ne všechny státy přistupují k vytvoření národní strategie stejným způsobem. Rostoucí počet a intenzita kybernetických útoků vyžadují bližší analýzu národních strategií kybernetické bezpečnosti.[6]

Úroveň vyspělosti národních strategií v oblasti kybernetické bezpečnosti se značně liší. Některé státy již vyvinuly sofistikovanější struktury řízení kybernetické bezpečnosti, zatímco jiné jsou stále ve fázi plánování bez ustálených standardů nebo metodik pro posouzení jejich efektivnosti. Rozvíjení dovedností, znalostí a osvědčených postupů v oblasti kybernetické bezpečnosti je cílem mnoha zemí, Turecko například zahrnuje vytvoření rozsáhlých osnov kybernetického vzdělávání v rámci svých vysokoškolských institucí.

Obecně se dá ale říci, že ústředním tématem každé národní strategie týkající se kybernetické bezpečnosti je odolnost, kterou můžeme definovat jako schopnost informačního systému nebo sítě nadále normálně fungovat navzdory útokům, jiným incidentům či technickým problémům. Strategie kybernetické bezpečnosti EU zahrnuje odolnost jako jednu ze svých pěti strategických priorit, ale bohužel neposkytuje jasné pokyny, jak je možné ji zajistit.[7]

Zdroje kybernetických hrozeb jsou blíže definovány jen v některých strategiích, ale obecně zahrnují hrozby pro národní bezpečnost, ekonomickou prosperitu, společenský blahobyt a kritickou infrastrukturu. Jak už bylo výše zmíněno, nejenom že se ve strategiích zpravidla neuvádí způsoby řešení problémů, ale většina strategií navíc nezahrnuje ani to, co považují za vážnou hrozbu, která by se mohla rovnat kybernetické válce nebo teroristickému útoku, ani to, jak se stávající strategie dokážou vypořádat s rychle se měnící dynamikou hrozeb. Národní strategie se nezabývají ani politikami nebo právními předpisy, které jsou potřebné k řešení a prevenci těchto útoků. Například Strategie kybernetické bezpečnosti Spojeného

[6] Greiman, VA. "Cybersecurity and Global Governance." Journal of Information Warfare 14, no. 4 (2015): 1–14. https://www.jstor.org/stable/26487502. str 2.
[7] Greiman, VA. "Cybersecurity And Global Governance." Journal Of Information Warfare 14, No. 4 (2015): 1–14. Https://Www.Jstor.Org/Stable/26487502. str 6.

království z roku 2011 zmiňuje jako jednu z potenciálních hrozeb možnost, že by státy mohly šířit dezinformace nebo teroristé mohli využívat kyberprostor k propagandě, radikalizovat potenciální příznivce či získávat finanční prostředky na své aktivity, ale strategie dále neposkytuje zastřešující právní rámec pro kontrolu těchto útoků.[8]

Většina strategií také uznává, že kyberprostor je z velké části vlastněn a provozován soukromým sektorem a že regulace by měly být založeny na spolupráci veřejného a soukromého sektoru, který může zahrnovat podniky, občanskou společnost anebo i akademickou obec. Ne všechny strategie však na tento aspekt kladou důraz a jen málo z nich jasně popisuje, jak by se spolupráce veřejného a soukromého sektoru měla rozvíjet, kdo by měl být do partnerství zapojen a jak bude v budoucnu řízena a kontrolována. Problematická je zde také skutečnost, že ač i soukromý sektor čelí kybernetickým hrozbám, je rozvrstven do tolika velikostí a typů, z nichž každá má jinou úroveň schopnosti řešit tyto hrozby, že je velice složité prosadit regulace, které by vyhovovaly všem. Nabízí se zde však také například myšlenka, že pokud jsou firmy příliš malé na to, aby si dostatečně zajistily ochranu proti kybernetickým útokům samy, mohly by benefitovat z nějaké formy koordinace kybernetické bezpečnosti s většími firmami v rámci stejného nebo podobného odvětví.

Národní strategie kybernetické bezpečnosti také vyzdvihují důležitost mezinárodního rozměru kybernetické bezpečnosti a potřebu lepších aliancí a partnerství s podobně smýšlejícími zeměmi nebo spojenci, včetně podporování méně rozvinutých zemí. Většina strategií však opět poskytuje jen málo podrobností o tom, jak dosáhnout vytyčených mezinárodních cílů, s výjimkou Spojených států, které vypracovaly konkrétní mezinárodní strategii pro kyberprostor a Spojeného království, které iniciovalo mezinárodní dialog na londýnské konferenci o kyberprostoru v listopadu 2011 s cílem podpořit mezinárodní normy týkající se chování v kyberprostoru.[9]

Často se také poukazuje na potřebu vyšší míry harmonizace právních předpisů proti kybernetické kriminalitě. Ta byla právně ukotvena Úmluvou o počítačové kriminalitě v roce 2001, podepsané v Budapešti. Jedná se tak o první mezinárodní smlouvu o

[8] The 2011 UK Cybersecurity Strategy
[9] Bílý dům 2011, UK Cabinet Office 2011

internetových zločinech.[10] Z 51 signatářů, kteří jí podepsali, Úmluvu ratifikovalo 39 států, včetně Spojených států a Velké Británie. Úmluva je často uváděna jako dobrý příklad harmonizace, přesto většina světa úmluvu neratifikovala, tím pádem má jen omezenou uplatnitelnost při řešení problémů, které souvisí s rozvojem struktury kybernetické správy. Bez všeobecné právní úpravy lze jen těžko najít řešení, které by odpovídalo různým přístupům ke kybernetické bezpečnosti po celém světě. Je také pozoruhodné, že v úmluvě ani v národních strategiích kybernetické bezpečnosti není žádná definice kybernetické trestné činnosti.

Nabízí se také otázka, zda by více pro vypracování mezinárodních kybernetických norem a pravidel nebylo možné udělat prostřednictvím mezinárodních organizací, jako například OSN. Diplomatické iniciativy, jako je například Finanční akční výbor OECD, využívají mezinárodní standardy k tomu, aby přiměly země zlepšit své reakční mechanismy ohledně praní špinavých peněz. Podobné iniciativy, jako je například Akční výbor pro kybernetickou bezpečnost, by mohly přinést konkrétnější výsledky v kybernetické oblasti. Snahu zabývat se touto problematikou můžeme zaznamenat i v NATO.[11]

1.2 Útoky v kyberprostoru a kybernetické hrozby

Čím vyspělejší společnost je, tím větší bývá její digitalizace a závislost na kyberprostoru. Vzhledem k této závislosti jsou státy mimořádně náchylné k interním či externím kybernetickým útokům a útokům na informační systémy. Vytváří se tím zcela nová zranitelná místa, jak pro státy jako takové, tak pro celou společnost. Ačkoli v celé historii internetu není známo, že by nějaký kybernetický útok zabil lidskou bytost a ani žádný stát otevřeně nevyhlásil kybernetickou válku nebo se přiznal ke sponzorování kybernetického útoku, škody způsobené v kyberprostoru prudce narůstají.[12]

Patří sem fyzické vyřazení nebo zničení počítačů, sítí, ekonomické ztráty v důsledku kybernetické kriminality a krádeže duševního vlastnictví, které se celosvětově odhadují na

[10] Sdělení č. 104/2013 Sb. m. s.; Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě dostupné z: 104/2013 Sb. m. s. Úmluva o počítačové kriminalitě (zakonyprolidi.cz) (staženo 10. 5. 2023).
[11] "Financial Action Task Force." FinCEN, https://www.fincen.gov/resources/international/financial-action-task-force (staženo 11. 5. 2023).
[12] Martin Libicki, Cyberdeterrence and Cyberwar, Santa Monica, Calif.: RAND Corporation, MG-877, 2009, str. 112.

nejméně 345 miliard dolarů ročně.[13] Tyto ztráty přiměly soukromé společnosti, vlády i jednotlivce, aby více investovali do prevence budoucích útoků. Aktuálně se celosvětové výdaje na kybernetickou bezpečnost odhadují na asi 70 miliard dolarů ročně.[14]

Obzvláště zrádnou charakteristikou kyberprostoru a útoků v nich je, že kybernetické útoky překračují státní hranice. Díky tomu je mimořádně těžké vysledovat jejich původ. Armády, teroristické skupiny a dokonce i jednotlivci mají nyní možnost zahájit kybernetické útoky, a to nejen proti vojenským sítím, ale i proti kritickým infrastrukturám, které jsou na počítačových sítích závislé. Současný svět je plný případů, kdy došlo k narušení soukromé a veřejné komunikace, manipulaci s bankovními systémy či dokonce zničení vojenských komunikačních systémů.

Na tomto místě můžeme uvést několik příkladů kybernetických konfliktů z nedávné doby, které názorně ilustrují výzvy, kterým státy v kyberprostoru v současnosti čelí.
V dubnu 2007 vyvolalo rozhodnutí estonské vlády přesunout válečný památník ze sovětské éry, bronzového vojáka, kybernetický konflikt v podobě třítýdenní vlny útoků typu Distributed Denial-of-Service (DDOS), které ochromily infrastrukturu informačních technologií v zemi.[15]

Kybernetické útoky dočasně narušily estonské komunikační sítě tím, že se zaměřily na vládu, noviny, mobilní telefony, systémy reakce na mimořádné události a banky. Cílem byl i estonský parlament a mnoho vládních ministerstev. Ačkoli kybernetické útoky nelze připsat konkrétnímu aktérovi, v Estonsku se všeobecně věří, že za těmito útoky stála Moskva. Rusko tvrdilo, že útoky pocházejí od kybernetických patriotů, a nikoli z rozkazu ruské vlády. [16]

Ať už je pravda kdekoli, je důležité si uvědomit, že je to právě neschopnost přičtení odpovědnosti za tyto typy útoků, které státům zamezují se efektivně bránit, jelikož by

[13] "Net Losses: Estimating the Global Cost of Cybercrime." Center for Strategic and International Studies, 5. 6. 2014, https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime (staženo 11. 5. 2023).
[14] Dobbins, James, et al. “Cybersecurity.” Choices for America in a Turbulent World: Strategic Rethink, RAND Corporation, 2015, str. 57–68. JSTOR, http://www.jstor.org/stable/10.7249/j.ctt17mvhfj
[15] Blank, S 2008, ‘Web war I: is Europe’s first information war a new kind of war?’, Comparative Strategy, vol. 27, no. 3, str. 227-47.
[16] Crosston, M 2011, ‘World gone cyber MAD: how mutually assured debilitation is the best hope for cyber deterrence’, Strategic Studies Quarterly, vol. 5, no. 1, str. 100-16.

mohly dle mezinárodního práva být v takovém případě za agresora označovány tyto státy samy.

Stejně tak během konfliktu, který vypukl o rok později, v srpnu 2008 mezi Ruskem a Gruzií ohledně Jižní Osetie, byly zahájeny kybernetické útoky proti gruzínským vládním webovým stránkám, médiím a komunikačním službám. Stejně jako v případě Estonska neexistuje důkaz o tom, kdo za těmito útoky stál. Gruzínský případ jasně ukazuje, že při kybernetických útocích, které se odehrávají ve světě bez hranic nelze uplatnit tradiční právo, které platí v případě ozbrojeného konfliktu. Situaci stěžuje i to, že překážky vstupu do kyberprostoru se rapidně snižují, především kvůli šíření nízkonákladových informačních a komunikačních technologií. Vedení kybernetických útoků se proto zdá být velmi atraktivní a méně nákladnou možností ve srovnání s použitím tradičních vojenských prostředků.[17]

Dalšími příklady kybernetických útoků a toho, že mohou mít mnoho podob, mohou být případy Ghost Netu a hackerských útoků na Google. Oba incidenty se týkaly Číny a vyvolávají mnoho otázek ohledně způsobu, jakým by oběti těchto útoků mohly reagovat. Ghost Net byla masivní kyberšpionážní operace, kterou objevil Information Warfare Monitor v březnu 2009. Operace použila malware a zaútočila na nevládní organizace a velvyslanectví zabývající se tibetskou problematikou ve103 zemích. V lednu 2010 Google oznámil, že počítačový útok pocházející z Číny pronikl do jeho firemní infrastruktury a ukradl informace z jeho počítačů, s největší pravděpodobností zdrojový kód. Útoky se také zaměřily na Gmailové účty lidskoprávních aktivistů a infiltrovaly sítě 33 společností.[18]

Nejnovějším a pravděpodobně nejvíce diskutovaným kybernetickým útokem je červ Stuxnet. Stuxnet je škodlivý software (lépe řečeno malware), který byl navržen speciálně pro útok na íránské jaderné zařízení v Natanzu v Iránu. Šířil se přes Microsoft Windows a zaměřil se na průmyslový software Siemens. Škodlivost Stuxnetu nespočívá ani tak v jeho technických vlastnostech, ale spíše v politickém a strategickém kontextu, v němž se objevil. Scénář preventivního úderu s cílem zastavit nebo zpomalit íránský jaderný program znepokojoval bezpečnostní experty již dlouhou dobu. Výsledek takové operace by

[17] Korns, S & Kastenberg, J 2009, 'Georgia's cyber left hook', Parameters, vol. 38, no. 4, str. 60-76.
[18]Klimburg, A. 2011, 'Mobilizing cyber power', Survival, vol. 53, no. 1, str. 41-60.

byl nejistý a rizika pro regionální a mezinárodní bezpečnosti potenciálně katastrofální. Preventivní úder konvenčními prostředky na íránská jaderná zařízení by s největší pravděpodobností rozpoutal konflikt na Blízkém východě a pravděpodobně by nezabránil případnému získání jaderných zbraní Íránem. Využití Stuxnetu ale představilo naprosto nové možnosti.[19]

Výše zmíněné útoky dokazují, že aktéři, státní i nestátní, mají schopnost kompromitovat a ovládat miliony počítačů, které patří vládám, soukromým podnikům a běžným občanům. Tento vývoj zapříčinil prudký nárůst zájmu o kybernetický prostor. Státní suverenita do značné míry definuje současný mezinárodní řád. Samotná Organizace spojených národů je založena na principu svrchované rovnosti všech svých členů a zachování státní suverenity je nejvyšší prioritou jak pro mezinárodní organizace, tak pro jednotlivé státy.

I díky tomu stále roste počet států, které se pokoušejí kontrolovat přístup svých občanů k informacím na základě toho, že určité typy obsahu představují hrozbu pro domácí pořádek nebo národní bezpečnost. Jako časté ospravedlnění takových praktik slouží například hrozba terorismu. Řada států, především členské státy USA a EU, zvýšily své filtrační sledovací techniky a omezily anonymitu v kyberprostoru. Avšak stále většina oficiálních strategií považuje potřebu respektování základních hodnot, jako je svoboda projevu, ochrana soukromí a volný tok informací, jako zásadní. Například britská strategie z roku 2011 zdůrazňuje, že kroky k posílení národní bezpečnosti musí být v souladu se základními právy občanů, jako je svoboda projevu, právo vyhledávat informace či právo na soukromí.[20]

1.3 Efektivní kybernetická bezpečnost

Úspěšná kybernetická bezpečnost ve své podstatě znamená umět dobře využívat jak ofenzivní, tak defenzivní kybernetické prostředky. Útočné kybernetické prostředky, jako je například hackerský útok nebo instalace malwaru, mohou ochromit nebo odvrátit možné kybernetické hrozby a mohou sloužit také jako odstrašující prostředek. Defenzivní stránka

[19] Josh Fruhlinger, "Stuxnet explained: The first known cyberweapon", CSO, 31. 8. 2022, https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html (staženo 11. 5. 2023).
[20] "The UK Cybersecurity Strategy", Cabinet Office, duben 2016, https://assets.publishing.service.gov.uk/media/5a81bae5e5274a2e8ab558ca/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (staženo 11. 5. 2023).

kybernetické bezpečnosti zahrnuje tvorbu národních kybernetických strategií a přijetí potřebných opatření pro boj proti kybernetické kriminalitě. V tomto hrají důležitou roli mezinárodně uznávané programy kybernetické bezpečnosti, jako je britské Národní centrum kybernetické bezpečnosti nebo Estonia Cooperative Cyber Defense Centre of Excellence, které usnadňují získávání znalostí o aktuálních bezpečnostních standardech, hrozbách a pomáhají při koordinaci akcí.[21]

Kybernetická bezpečnost se tedy zaměřuje na dvě hlavní témata. Prvním jsou poměrné běžné útoky pomocí šíření malwaru, se kterými se státy setkávají každý den. Druhým, značně závažnějším je scénář, kdy hrozí kybernetický útok na kritickou infrastrukturu nebo vládní subjekty. Defenzivní aspekt kybernetické bezpečnosti by se měl posuzovat jak podle schopnosti zabránit každodenní škodlivé činnosti, nebo ji alespoň výrazně omezit, tak podle připravenosti na možný větší kybernetický útok.

Kybernetický prostor lze rozdělit na tři vzájemně propojené vrstvy - fyzickou vrstvu, logickou vrstvu a vrstvu kybernetické osobnosti. Při plánování je třeba brát v úvahu interakce mezi těmito vrstvami a také mezi soukromou a veřejnou doménou. Fyzickou vrstvu tvoří IT zařízení a infrastruktura v reálném světě, zatímco logická síťová vrstva se týká dat, programování a kódu, které tvoří kyberprostor. Přenos informací je často umožněn díky výsledkům právě z fyzické vrstvy, které mohou být reprezentovány jedinou adresou URL.[22]

Třetí vrstva, kybernetické osobnosti, se vztahuje na osoby nebo subjekty působící v kyberprostoru, ať už lidské nebo automatizované. Všechny tyto vrstvy jsou nezbytné pro každou kybernetickou operaci, kde útok nebo narušení jedné sítě ohrožuje všechny ostatní. V zájmu národní bezpečnosti by počítačové komponenty ve fyzické sféře měly pocházet z důvěryhodných zdrojů, přičemž se řeší i obavy o údaje jednotlivých spotřebitelů v případě narušení kybernetické bezpečnosti firem. Efektivní kybernetická bezpečnost zahrnuje

[21] Pendino, Stephanie LCDR, Jahn, Robert K. MAJ, Sr., a Pedersen, Kirk Mr.„U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light." *Joint Forces Staff College*, 7. 9. 2022. https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/ (staženo 10. 5. 2023).

[22] Price, Sean K, "Perfidy in Cyberspace: The Requirement for Human Confidence", *Harvard National Security Journal*, 21. 2. 2020, https://harvardnsj.org/2020/02/21/perfidy-in-cyberspace-the-requirement-for-human-confidence/ (staženo 10. 5. 2023).

všechny tyto proměnné do svého plánování.[23]

Efektivní kybernetická bezpečnost zahrnuje také pravidelné hodnocení rizik a testování zranitelných míst, aby bylo možné identifikovat a řešit potenciální bezpečnostní nedostatky. Tato hodnocení by měla probíhat průběžně a měla by reagovat na nové hrozby, jakmile se objeví. Kromě technických opatření se dobrá kybernetická bezpečnost do značné míry opírá o programy zvyšující kybernetickou gramotnost a zvyšování obecného povědomí zaměstnanců a uživatelů, protože lidský faktor je často významnou slabinou bezpečnostních systémů. Toto školení by mělo zahrnovat témata, jako je rozpoznávání pokusů o phishing, postupy bezpečného prohlížení stránek a vytváření silných hesel.

V květnu 2018 vstoupilo v platnost obecné nařízení Evropské unie o ochraně osobních údajů (GDPR), které pro firmy působící v EU znamená revoluci v používání dat. Porušení nařízení GDPR může vést k pokutám a pošpinění dobrého jména společnosti, kdy ztratí důvěru svých zákazníků. Kybernetická bezpečnost má zásadní význam pro prevenci ztráty dat a jejich narušení. Společnost Mandiant (později přejmenována na FireEye), která se zabývá kybernetickou bezpečností, poskytla soubor osvědčených postupů pro společnosti, které mají za cíl zlepšit jejich kybernetickou bezpečnost. Jako nejdůležitější se podle manuálu jeví vytvoření týmů pro reakci na kybernetické incidenty (CIRT). Týmy CIRT spolu často spolupracují za účelem vzájemného prospěchu, například sdílení znalostí o incidentech, a posilují tak standardy kybernetické bezpečnosti.[24]

Například Dánsko, které je často považováno za zemi s nejlepší kybernetickou bezpečností klade velký důraz na rozvoj znalostí o kybernetické bezpečnosti mezi občany, soukromým sektorem i úřady. Země vykazuje nejnižší počet finančních malwarových útoků a počítačových malwarových infekcí napříč celou společností, což svědčí o úspěchu dánské

[23] Price, Sean K. "Perfidy in Cyberspace: The Requirement for Human Confidence", *Harvard National Security Journal*, 21. 2. 2020. https://harvardnsj.org/2020/02/21/perfidy-in-cyberspace-the-requirement-for-human-confidence/ (staženo 10. 5. 2023).

[24] Wolford, Ben. "What is GDPR, the EU's new data protection law?" *GDPR.eu*. https://gdpr.eu/what-is-gdpr/ (staženo 10. 5. 2023).

Ferrillo, Paul. "The Importance of a Battle-Tested Cyber Incident Response Plan." *Harvard Law School Forum on Corporate Governance*, 19. 12. 2014. https://corpgov.law.harvard.edu/2014/12/19/the-importance-of-a-battle-tested-cyber-incident-response-plan/ (staženo 10. 5. 2023).

vlády při šíření povědomí o kybernetických hrozbách.[25]

2. Historický vývoj strategií kybernetické bezpečnosti

Jak Spojené státy, tak a Spojené království provedly některé úpravy v reakci na technologické změny. Zatímco některé obranné funkce lze snadno přizpůsobit stávajícím vládním institucím a právním rámcům, jiné představují složitější výzvu z hlediska institucionálního uspořádání a právní architektury.

Obě země mají dobře fungující obranné složky, jako jsou kontrarozvědka a vojenská obrana, které se řídí podle zavedených norem a právních rámců. Rychlý rozvoj kybernetické oblasti si však vyžádal přizpůsobení těchto struktur měnící se povaze mezistátních interakcí a obavám o národní bezpečnost. Technologický pokrok často vyžaduje vytvoření zcela nových norem, které odrážejí nové problémy, které se v kyberprostoru vyskytly. Tak tomu bylo ostatně v každé z domén, ve kterých státy chrání své zájmy. Jako tomu bylo v případě rozvoje letectví, kdy pokoření této domény vedlo k vytvoření leteckých sil a mezinárodních leteckých dohod, podobně i kybernetická oblast si vyžádala vytvoření specializovaných institucí a právních rámců, které by se vypořádaly se specifickými výzvami, jež přináší.[26]

K faktorům, které dělají kyberprostor tak unikátním, patří například fakt, že již při útocích nehraje roli fyzická blízkost. Dále je velmi obtížné určit, kdo je za útok v kyberprostoru zodpovědný, ať už se jedná o jednotlivce, anebo státy. Rychlost a rozsah operací, zranitelnost dat a systémů vůči krádeži nebo zničení, cenová dostupnost rozvoje vládních kybernetických schopností, dostupnost hackerských nástrojů na černém trhu a schopnost soukromých subjektů vstoupit do kyberprostoru jsou všechno faktory, které musíme vést v patrnosti.

[25] Venkina, Ekaterina, "How Denmark became the most cyber-secure country", *IPS Journal*, 20. 6. 2021, https://www.ips-journal.eu/work-and-digitalisation/how-denmark-became-the-most-cyber-secure-country-5290/ (staženo 13. 9. 2023).
[26] "The Evolution of Cybersecurity in the UK vs. US.". VirtualArmour Team. *VirtualArmour*, 28. 2. 2017, https://virtualarmour.com/the-evolution-of-cybersecurity-in-the-uk-vs-us/ (staženo 13. 9. 2023).

Tyto prvky dohromady vytvářejí prostředí, ve kterém má více aktérů možnost zapojit se do špionáže, krádeží a manipulace s cennými aktivy. Vlády musí přizpůsobit své instituce a právní rámce tak, aby se účinně bránily těmto rizikům a využívaly příležitostí, které kybernetická oblast nabízí. Neustále se vyvíjející povaha kybernetické oblasti vyžaduje neustálé přizpůsobování, chceme-li účinně zachovat národní bezpečnost.
Oba zkoumané státy si uvědomují potřebu chránit informační systémy a s nimi související data, zejména ty, které jsou spojeny s vládou a kritickou infrastrukturou. Ačkoli se způsoby, kterými se toho snaží dosáhnout často liší, jejich cíle se shodují.

Díky schopnosti Národní bezpečnostní agentury (NSA) a ministerstva obrany účinně reorganizovat svou strukturu, můžeme již teď pozorovat značný pokrok v zabezpečení systémů národní bezpečnosti spojených s vojenskými a zpravodajskými aktivitami. Je však evidentní, že se pokroku zatím nedočkaly všechny sféry národní bezpečnosti. Zatímco u systémů národní bezpečnosti probíhá bezpečnostní pokrok rychleji, rozšíření kybernetických bezpečnostních opatření do jiných oblastí stále představuje výzvu. Koordinaci brání mimo jiné taky fakt, že neexistuje jedna instituce, která by zaštiťovala všechny vládní resorty.[27]

Model Spojeného království se od modelu USA liší z hlediska formálních institucionálních struktur a také v tom, jakou roli by měly mít zpravodajské služby. Obě země se zaměřují na obranná opatření na ochranu svých systémů a také poskytují podporu soukromému sektoru v oblasti kybernetické bezpečnosti. V posledních letech došlo k vytvoření nových organizací se specifickými funkcemi, které odrážejí jak změny ve státním, tak v soukromém sektoru. Řeší se však i ofenzivní činnosti, jako je prosazování práva, špionáž a ozbrojený konflikt v kyberprostoru. Obě vlády vyvinuly své ofenzivní strategie takovým způsobem, aby nebylo možné je označit za důvod k válce, ale zároveň bylo možné se účinně bránit.

2.1 Vývoj strategií kybernetické bezpečnosti v USA

V 80. letech minulého století, začala Národní bezpečnostní agentura (NSA) rozšiřovat své

[27]“ Fact Sheet: 2023 DoD Cyber Strategy“, US Department of Defence, květen 2023. https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF#:~:text=2023%20DoD%20Cyber%20Strategy,It%20complements%20the (staženo 15. 9. 2023).

služby v oblasti informační bezpečnosti v rámci celého ministerstva obrany. Navzdory počátečnímu odporu převzala NSA klíčovou roli při stanovování bezpečnostních standardů pro takzvané národní bezpečnostní systémy. Kongres však zabránil tomu, aby NSA rozšířila svou působnost napříč ostatními ministerstvy. Ředitelství NSA pro zajištění informací zajišťuje bezpečnostní funkce pro utajované systémy národní bezpečnosti. Avšak cvičení Eligible Receiver v roce 1997 odhalilo špatnou připravenost ministerstva obrany na selhání jeho kybernetické bezpečnosti, což dokázalo, že je na čase rozšířit bezpečností struktury i do oblastí, které byly mimo působnost NSA. Toto mělo za následek vytvoření Joint Task Force-Computer Network Defense (JTF-CND), která měla tyto nedostatky řešit. JTF-CND sloučila operační funkce zaměřené na obranu a zpočátku se soustředila na monitorování sítí. Působnost JTF-CND se nakonec rozšířila i na útoky na počítačové sítě.[28]

V průběhu času JTF-CND, prošla významnými změnami a nakonec se transformovala do kybernetického velitelství USA (USCYBERCOM). Tato transformace zahrnovala sloučení USCYBERCOM s Národní bezpečnostní agenturou (NSA) za účelem inkubace. Díky sdílení společného vedení a základně ve stejném místě, získal USCYBERCOM přístup k personálu a technické infrastruktuře NSA, což umožnilo rychlý nárůst jeho schopností pro obranné i útočné kybernetické mise. USCYBERCOM se vyvinul v plnohodnotné bojové velitelství a aktuálně čelí stále probíhajícím debatám o přerušení dvojího vztahu s NSA. Nicméně vytvořil dobře rozvinutou institucionální strukturu pro obranné mise ministerstva obrany prostřednictvím podřízeného velitelství s názvem Joint Force Headquarters-DoD Information Network (JFHQ-DoDIN). JFHQ-DoDIN slouží jako centralizovaný mechanismus pro politiku řízení rizik kybernetické bezpečnosti, dohled nad dodržováním předpisů, vydávání směrnic, poskytování centrálních operačních obranných služeb a nasazování personálu označovaných jako týmy kybernetické ochrany v případech, kdy vlastní kapacity obranných organizací ministerstva obrany nejsou dostatečné.[29]

Zatímco ve vojenské a zpravodajské komunitě bylo v oblasti kybernetické bezpečnosti

[28] Michael Martelle, "Eligible Receiver 97: Seminal DOD Cyber Exercise Included Mock Terror Strikes and Hostage Simulations," National Security Archive, 1. 8. 2018, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations staženo (15. 9. 2023).
[29] "History of U.S. Cyber Command", U.S. Cyber Command, https://www.cybercom.mil/About/History/. (staženo 15. 9. 2023).

dosaženo značného pokroku, v organizacích federální vlády mimo tyto sektory, souhrnně označovaných jako federální civilní výkonná složka (FCEB), docházelo k pomalejším změnám.

V roce 1996 učinil Kongres první krok tím, že pro FCEB zřídil funkci stanovování norem a pověřil touto odpovědností ministra obchodu. Národní institut pro standardy a technologie (NIST) byl pověřen zajištěním potřebných odborných znalostí pro tvorbu standardů kybernetické bezpečnosti. Kongres však nepověřil žádný subjekt, který by dodržování těchto norem vymáhal prostřednictvím auditu. Krátce poté bylo navrženo centralizovat síťovou infrastrukturu FCEB s cílem posílit možnosti monitorování, případně zapojit Národní bezpečnostní agenturu (NSA). Tento návrh se setkal s odporem, neboť mnozí považovali kybernetickou bezpečnost za aspekt řízení informačních technologií, který je lepší ponechat na jednotlivých agenturách. K odporu přispěly i obavy o ochranu soukromí, což nakonec vedlo k neúspěchu návrhu.[30]

V roce 2002 Kongres přijal zákon o řízení bezpečnosti informací (Federal Information Security Management Act - FISMA), který přinesl zlepšení procesu stanovování norem. Odpovědnost za vyhlašování standardů založených na NIST přešla z ministerstva obchodu na Úřad pro řízení a rozpočet (OMB) Bílého domu a OMB získal pravomoc kontrolovat jejich dodržování v ostatních agenturách. FISMA rovněž nařídila vytvoření US-CERT (Computer Emergency Readiness Team), který poskytoval FCEB odborné poradenství v oblasti kybernetické bezpečnosti, a to jak v rámci preventivních opatření, tak při reakci na útoky. Ačkoli US-CERT neposkytoval centralizované bezpečnostní služby, představoval významný krok směrem k možnosti centralizace.

Následovaly další pokroky, včetně zřízení ministerstva vnitřní bezpečnosti v roce 2008. Národní ředitelství pro ochranu a programy (National Protection and Programs Directorate - NPPD), součást DHS, převzalo odpovědnost za fyzickou bezpečnost a kybernetickou bezpečnost soukromé kritické infrastruktury a FCEB. V rámci NPPD byl umístěn US-CERT a prezident Bush nařídil vytvoření schopnosti detekce hrozeb nazvané "EINSTEIN".

[30] James Olthoff, "Setting the Standards: Strengthening U.S. Leadership in Technical Standards," National Institute of Standards and Technology, 17. 3. 2022, https://www.nist.gov/speech-testimony/setting-standards-strengthening-us-leadership-technical-standards (staženo 17. 9. 2023).

Tento senzorový systém založený na signaturách monitoroval síťový provoz a hledal indikátory kompromitace, čímž posílil obranné služby FCEB.[31]

V roce 2010 prezident Obama nařídil Úřadu pro řízení a rozpočet, aby delegoval svou funkci kontroly dodržování předpisů na nově zřízené Národní ředitelství pro ochranu a programy (NPPD) Ministerstva vnitřní bezpečnosti. Tímto krokem bylo NPPD pověřeno dohledem nad dodržováním standardů Národního institutu pro standardy a technologie (NIST) v oblasti FCEB. V roce 2014 Kongres v rámci významné aktualizace federálního zákona o řízení bezpečnosti informací (FISMA) udělil NPPD pravomoc vydávat takzvané závazné provozní směrnice, které mají zajistit, aby subjekty FCEB přijaly konkrétní opatření v reakci na známá slabá místa a rizika v oblasti bezpečnosti informací. Tato pravomoc řešila předchozí omezení NPPD, kterému chyběly donucovací pravomoci a přímé prostředky k postihu subjektů, které nedodržují předpisy.

To se záhy ukázalo jako velmi užitečné, když NPPD vyvinul program, který skenoval systémy FCEB, uměl odhalit zranitelná místa a zprávy o nich poskytoval příslušným agenturám. Ty však tato doporučení dostatečně nevyužívaly, anebo úplně ignorovaly. S pravomocí vydávat závazné provozní směrnice by nyní NPPD mohl agentury donutit, aby na základě oznámení o kritických zranitelnostech ve stanoveném časovém rámci minimálně jednaly.[32]

Kongres dále rozšířil pravomoci NPPD tím, že umožnil vydávání nouzových směrnic v reakci na hrozby pro bezpečnost informací. Tato kapacita umožnila vedoucímu agentury FCEB rychle jednat a řešit nově vznikající rizika. V rámci této pozoruhodné transformace bylo Národní ředitelství pro ochranu a programy (NPPD) koncem roku 2018

[31] Federal Information Security Modernization Act. "Cybersecurity & Infrastructure Security Agency". 'https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act. (staženo 17. 9. 2023).
Moteff, John D. "Critical Infrastructures: Background, Policy, and Implementation". 10. 6. 2015. Congressional Research Service. https://sgp.fas.org/crs/homesec/RL30153.pdf str. 6 (staženo 17. 9. 2023).
[32] Federal Information Security Modernization Act. "Cybersecurity & Infrastructure Security Agency". 'https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act. (staženo 17. 9. 2023).
Ann Barron-DiCamillo, "Written testimony of NPPD for a House Committee on Oversight and Government Reform hearing titled 'Examining ObamaCare's Failures in Security, Accountability, and Transparency'," Department of Homeland Security, 18. 9. 2014, https://www.dhs.gov/news/2014/09/18/written-testimony-nppd-house-committee-oversight-and-government-reform-hearing. (staženo 20. 9. 2023).

přejmenováno na Agenturu pro kybernetickou bezpečnost a bezpečnost infrastruktury (CISA). Tato změna jména, ačkoli zdánlivě nenápadná, přispěla k jasnějšímu pochopení úlohy CISA a pomohla upevnit její poslání v rámci FCEB a soukromého sektoru.[33]

Během následujících dvou let CISA rozšířila své obranné služby a nabídla FCEB, vládním subjektům a soukromým subjektům kritické infrastruktury pomoc při vyhledávání hrozeb, reakci na incidenty, průběžnou diagnostiku, skenování zranitelností a další funkce. Navzdory těmto pokrokům se však CISA stále potýkala s finančními omezeními, která omezovala rozsah její činnosti v rámci FCEB.

Za zmínku stojí také pokroky v rámci federální civilní výkonné moci a soukromé kritické infrastruktury. CISA, Agentura pro kybernetickou bezpečnost a bezpečnost infrastruktury, se v minulosti potýkala s omezeními při poskytování komplexních obranných služeb kvůli dvěma hlavním problémům. Zaprvé jí chyběly potřebné pravomoci, aby mohla svou pomoc nabízet v širším měřítku. Za druhé, její služby subjektům FCEB byly zcela dobrovolné a vyžadovaly souhlas každého jednotlivého subjektu. Například vyhledávání hrozeb se uskutečňovalo pouze na základě konkrétních žádostí.

Nedávné právní předpisy však přinesly významné změny. V prosinci 2020 Kongres v rámci zákona o autorizaci národní obrany na fiskální rok 2021 přijal článek 1705, který CISA výslovně zmocňuje k provádění operací vyhledávání hrozeb v informačních systémech agentur FCEB, s jejich předchozím oznámením nebo bez jejich povolení. To znamená odklon od dobrovolného přístupu a dává CISA pravomoc jednat proaktivně při ochraně agentur FCEB. Ačkoli vládní obranné služby v rámci FCEB ještě nejsou plně centralizovány, posílená pravomoc CISA, včetně možnosti vydávat závazné operační směrnice a nouzové směrnice, poskytla podstatně silnější základ. Tyto změny přišly v klíčovou dobu vzhledem k významnému dopadu nedávných narušení kybernetické bezpečnosti. Je však důležité poznamenat, že účinnost a rozšiřitelnost těchto pravomocí závisí na dostatečných rozpočtových a personálních zdrojích.[34]

[33] "Cybersecurity and Infrastructure Security Agency," Cybersecurity & Infrastructure Security Agency, naposledy upraveno 20. 11. 2018, https://www.cisa.gov/news-events/alerts/2018/11/19/cybersecurity-and-infrastructure-security-agency (staženo 20. 9. 2023).

[34] "The U.S. National Defense Authorization Act for Fiscal Year 2021: Cybersecurity Provisions". Mayer Brown. Lexology. https://www.lexology.com/library/detail.aspx?g=b3332196-151c-4ae0-a800-

Pokud jde o bezpečnost soukromé kritické infrastruktury, od poloviny 90. let výrazně vzrostl zájem federální vlády na jejím posílení. Po bombovém útoku v Oklahoma City v roce 1995 zřídil prezident Bill Clinton pracovní skupinu pro kritickou infrastrukturu, která se zabývala bezpečnostními problémy. Tato skupina uznala zranitelnost kritické infrastruktury v oblasti kybernetické bezpečnosti a zdůraznila potřebu zásahů.[35]

Slyšení kongresového výboru v roce 1996 poukázalo na několik problémů při zlepšování kybernetické bezpečnosti v oblasti kritické infrastruktury. Mezi tyto problémy patřila neochota soukromého sektoru přijímat opatření, která by mohla narušit konkurenční výhodu, nejistota v oblasti atribuce, nedůvěra v zapojení vlády, upřednostňování soukromých firem zabývajících se kybernetickou bezpečností, nedostatek spolehlivých předpovědí hrozeb a technických kapacit a další. V reakci na tyto problémy vytvořila Clintonova vláda komisi, jejímž úkolem bylo vypracovat řešení pro zvýšení kybernetické bezpečnosti v soukromém sektoru kritické infrastruktury.[36]

Tato komise, známá také jako prezidentská komise pro ochranu kritické infrastruktury, vypracovala v roce 1997 zprávu, která upozornila na hrozby pro kybernetickou bezpečnost kritické infrastruktury a poskytla doporučení pro její ochranu. Zpráva obhajovala partnerství veřejného a soukromého sektoru a dobrovolnou výměnu informací jako nejúčinnější a nejefektivnější přístup a upřednostňovala jej před legislativou nebo regulací.[37]

O rok později prezident Clinton v prezidentské směrnici 63 zdůraznil význam sdílení informací a modelu dobrovolného partnerství pro zlepšení kybernetické bezpečnosti kritické infrastruktury. Vyzývala k vytvoření národního plánu ochrany infrastruktury, zřízení funkce koordinátora v Bílém domě, vedoucích agentur pro jednotlivé sektory

bdc17e67d6e9#:~:text=Section%201705%20authorizes%20CISA%20to,vulnerabilities%20within%20Federal%20information (staženo 20. 9. 2023).

[35] Michael Hardy, "The wake-up call," Federal Times, 11. 7. 2016, https://www.federaltimes.com/smr/critical-infrastructure/2016/07/11/the-wake-up-call/ (staženo 20. 9. 2023).

[36] Marcus H. Sachs, "Reflections on Executive Order 13010," McCrary Institute, 15. 7. 2021, https://mccrary.auburn.edu/work/insights/reflections-on-executive-order-13010/ (staženo 21. 9. 2023).

[37] Ibidem.

kritické infrastruktury a určených úředníků a styčných osob ze soukromého sektoru, což by výrazně usnadnilo spolupráci. Výsledkem bylo zřízení center pro sdílení a analýzu informací, které usnadnilo lepší sdílení indikátorů hrozeb a užitečných informací.[38]

Národní strategie prezidenta Bushe pro bezpečnost kyberprostoru z roku 2003 se nadále zaměřovala na dobrovolné partnerství veřejného a soukromého sektoru a sdílení informací. Určila nově vytvořené ministerstvo vnitřní bezpečnosti (DHS) jako hlavní kontaktní místo pro interakci federální vlády s průmyslem a dalšími partnery, ale postrádala potřebné zdroje a povinné pravomoci k účinnému řešení rozsahu úkolu kybernetické bezpečnosti. V prvních letech Obamovy vlády zůstával federální přístup ke kybernetické bezpečnosti kritické infrastruktury soukromého sektoru relativně neměnný.

Počátkem roku 2013 však byly vydány exekutivní příkaz č. 13636 a prezidentská směrnice č. 21 (PPD-21), které přinesly změny. Cílem těchto směrnic bylo zvýšit kybernetickou bezpečnost kritické infrastruktury tím, že podpořily dobrovolné sdílení informací, nařídily Národnímu institutu pro standardy a technologie vypracovat rámec pro řízení rizik (tzv. rámec kybernetické bezpečnosti) a poskytly pokyny pro postupy, které už měly možnost ověřit.[39]

Během těchto pokroků byl důsledně kladen důraz na dobrovolnou spolupráci, sdílení informací a partnerství veřejného a soukromého sektoru. Zatím se nehovořilo se o regulačních nebo legislativních zásazích, které by soukromému sektoru vnucovaly pravidla kybernetické bezpečnosti nebo umožňovaly přímý přístup vlády do systémů soukromého sektoru.

Za Obamovy administrativy avšak proběhlo mnoho debat ohledně regulací i v soukromém sektoru. Výše zmíněný exekutivní případ a směrnice, měly za cíl zvýšit kybernetickou bezpečnost, ale nenutily vlastníky/provozovatele kritické infrastruktury v soukromém sektoru k přijetí konkrétních opatření. Soukromému sektoru toto nebylo možné nařídit bez

[38] "Presidential Decision Directive/NSC-63," Federation of American Scientists, 22. 5. 1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm (staženo 30. 9. 2023).
[39] "Cybersecurity & Infrastructure Security Agency, 'Executive Order 13636 and Presidential Policy Directive 21. CISA. https://www.cisa.gov/executive-order-13636-and-presidential-policy-directive-21. (staženo 30. 9. 2023).

příslušné legislativy. Obamova administrativa zkoumala možnost zavedení povinných standardů kybernetické bezpečnosti pro klíčové subjekty soukromého sektoru, ale tento návrh nepokročil.

Po přijetí zákona o sdílení informací o kybernetické bezpečnosti v roce 2015 oznámila administrativa další snahy o podporu kybernetické bezpečnosti, a to i v oblasti kritické infrastruktury. Byla zavedena opatření, jako je umožnění vlastníkům/provozovatelům kritické infrastruktury simulovat útoky na jejich systémy a poskytování jejího hodnocení na místě a podpory pro zlepšení. Transformace NPPD na CISA k tomuto výrazně přispěla.[40]

V roce 2017 vydala Trumpova administrativa exekutivní příkaz č. 13800, který nařídil přezkum stávajících regulačních orgánů pro kybernetickou bezpečnost v těch subjektech kritické infrastruktury, které jsou považovány za nejdůležitější. Cílem bylo identifikovat regulační pravomoci, které by mohly být užitečné pro zlepšení bezpečnosti. Výjimkou této regulace v soukromém sektoru je obranná průmyslová základna (DIB). V roce 2020 ministerstvo obrany využilo své páky na uzavírání smluv a přimělo společnosti DIB, aby zvýšily svou vlastní kybernetickou bezpečnost a prosadily lepší opatření v oblasti kybernetické bezpečnosti v rámci svých dodavatelských řetězců.[41]

Dříve měla pravidla pro akvizice DIB nominální požadavky, avšak chyběla účinná kontrola jejich dodržování. Systém Certifikace modelu vyspělosti kybernetické bezpečnosti (Cybersecurity Maturity Model Certification) vyžaduje, aby firmy splňovaly požadavky na kybernetickou bezpečnost odpovídající jejich rozsahu a sofistikovanosti, a musí získat osvědčení o jejich splnění od externího auditora. Ačkoli se zavedení tohoto systému může zpočátku potýkat s nějakými problémy, v případě úspěchu by se mohl stát

[40] "Cybersecurity & Infrastructure Security Agency, 'Cybersecurity Information Sharing Act of 2015 Procedures and Guidance". Naposledy upraveno 15. 10. 2021, https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance (staženo 2. 10. 2023).

[41] Wade H. Atkinson, Jr., "A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy," The Institute of World Politics, 22. 10. 2020, https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/ (staženo 2. 10. 2023).

užitečným manuálem, jak v budoucnu zlepšit kybernetickou bezpečnost kritické infrastruktury.[42]

Za zmínku stojí i vztah mezi USCYBERCOM a NSA, zejména pokud jde o jejich oddělené role a kompetence. Kritici tvrdí, že současné uspořádání nespravedlivě upřednostňuje ochranu při shromažďování zpravodajských informací ze strany NSA, která upřednostňuje monitorování před aktivním narušováním systémů protivníka. Někteří tvrdí, že má-li USCYBERCOM dosáhnout svého plného potenciálu, musí se oddělit od NSA.[43]

Tento argument podporovala i skutečnost, že během války proti Islámskému státu se objevily názory, že USCYBERCOM nebyl dostatečně agresivní při narušování jeho systémů, právě kvůli přílišnému důrazu na shromažďování zpravodajských informací. Tehdejší ministr obrany vyzval USCYBERCOM, aby prováděl více rušivých operací, což vyústilo v operaci známou jako Glowing Symphony. Výsledky těchto operací však nebyly zcela úspěšné, protože Islámský stát dokázal obnovit své systémy rychleji, než je Američané zvládali infiltrovat. Pro zastánce současného uspořádání toto byl dostatečný důkaz, že by měl převážit rovnoměrný přístup při shromažďování zpravodajských informací a ofenzivní politice, zatímco kritici v tom viděli důvod, proč prolomit zaběhnuté pořádky a umožnit USCYBERCOMu rozvinout své schopnosti mimo zaběhnutou strukturu.[44]

Operace Glowing Symphony také upozornila na složitější otázky související s mezinárodním právem, mezinárodními vztahy a napětím mezi bezpečnostními agenturami. V některých případech vyžadovaly kybernetické operace proti Islámskému státu přístup k systémům umístěným v třetích zemích, například v Německu. Ministerstvo zahraničí, CIA a FBI se obávaly, že provádění takových operací bez souhlasu zúčastněné země by mohlo mít negativní důsledky pro jejich budoucí spolupráci. Byly vzneseny také námitky na

[42] Uday Ali Pabrai, "US DoD Launches Comprehensive CMMC 2.0 Cybersecurity Framework," ISACA, 25. 1. 2022, https://www.isaca.org/resources/news-and-trends/industry-news/2022/us-dod-launches-comprehensive-cmmc-2-cybersecurity-framework (staženo 2. 10. 2023).
[43] Emma Kohse and Chris Mirasola, "To Split or Not to Split: The Future of CYBERCOM's Relationship with NSA," Lawfare, 12. 4. 2017, https://www.lawfaremedia.org/article/split-or-not-split-future-cybercoms-relationship-nsa (staženo 4. 10. 2023).
[44] "Operation Glowing Symphony (2016)," International Cyber Law: Interactive Toolkit, naposledy upraveno 4. 6. 2021, https://cyberlaw.ccdcoe.org/wiki/Operation_Glowing_Symphony_(2016) (staženo 4. 10. 2023).

základě mezinárodního práva a suverenity, přičemž se zpochybňovalo, zda operace na těchto serverech bez souhlasu států neporušují suverenitu příslušných zemí.[45]

Ve Spojených státech se vedlo také mnoho debat ohledně kompetencí USCYBERCOM, jelikož mnozí zastávali názor, že USCYBERCOM nemá pravomoc provádět operace ve třetích zemích, které porušují mezinárodní právo, na rozdíl od CIA. Pentagon však těmto pochybám oponoval tvrzením, že jeho plánované operace nebudou mít žádné významné vedlejší účinky na třetí země a že jeho stávající pravomoci jsou dostatečné pro pokrytí operací, které jsou prováděny bez upozornění třetích stran. Tento přístup však z hlediska etiky poněkud narušuje právo na suverenitu státu nad svým územím, i když se jedná o to v kyberprostoru.[46]

2.2 Vývoj strategií kybernetické bezpečnosti ve Spojeném království

Nárůst důležitosti kyberprostoru měl zásadní dopad na vládní komunikační centrálu (GCHQ) ve Spojeném království. Ačkoli komunikační technologie byly pro britskou Vládní komunikační centrálu vždy klíčové, během studené války se zaměřovala především na prolamování šifrování a ochranu informačního systému Spojeného království před nepřátelskými zpravodajskými službami. Myšlenka, že se národní zájmy budou nevyhnutelně prolínat právě s bezpečností počítačových systémů a sítí, nebyla zpočátku tak zřejmá, jako je tomu dnes. S výrazným přechodem na počítačové komunikační, obchodní a řídicí systémy však byla postupná změna priorit nevyhnutelná.

Podobně jako ve Spojených státech, i ve Velké Británii došlo v 90. letech ke změně pohledu na zranitelnost kritické infrastruktury. Incident z roku 1995, který zahrnoval vydírání finančních institucí v Londýně, ukázal potřebu odborných znalostí v oblasti kybernetické bezpečnosti i v soukromém sektoru. Jelikož Britská centrální banka, ani ministerstvo obchodu a průmyslu, které byly terči útoku, neměly potřebné odborné znalosti, do vyšetřování se zapojilo GCHQ. Na tomto incidentu lze dobře ilustrovat

[45] Michael Martelle, "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY," National Security Archive, 21. 1. 2020, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony (staženo 6. 10. 2023).
[46] Mark Pomerleau, "Cyber Command granted new, expanded authorities," C4ISRNET, 28. 2. 2018, https://www.c4isrnet.com/dod/cybercom/2018/02/28/cyber-command-granted-new-and-expanded-authorities/ (staženo 8. 10. 2023).

flexibilitu britského modelu, neboť využil forenzní odborné znalosti zpravodajské komunity v a aplikoval je mimo svůj sektor. GCHQ se od tohoto momentu podílela na spolupráci s různými složkami vlády i soukromého sektoru, kdy měla za úkol chránit elektronické systémy, které zajišťovaly nejdůležitější operce, včetně bankovnictví, obchodu a veřejných služeb.

Na konci 90. let si Spojené království, stejně jako Spojené státy, uvědomilo rostoucí hrozby pro kritickou národní infrastrukturu spojenou s kybernetickou bezpečností. To vedlo úředníky k úvahám, jak zefektivnit sdílení informací o hrozbách a rozšířit povědomí o osvědčených postupech, jak jim úspěšně čelit. Zatímco Spojené státy podporovaly vznik center pro sdílení a analýzu informací (ISAC) v soukromém sektoru, Spojené království udělalo další krok a vytvořilo nový vládní subjekt, který se věnuje podpoře iniciativ sdílení informací. V USA byl podobný subjekt zřízen až po vzniku ministerstva vnitřní bezpečnosti.[47]

V roce 1999 vláda vytvořila Národní koordinační centrum pro bezpečnost infrastruktury (NISCC), meziresortní organizaci, jejímž úkolem je poskytovat poradenství a včasné varování subjektů pro účinné odhalování hrozeb a lepší zajištění jejich systémů. NISCC využívalo kapacity různých vládních složek, včetně Skupiny pro bezpečnost komunikací a elektroniky (Communications-Electronics Security Group - CESG) GCHQ, která se původně zaměřovala na zajišťování informací pro obranné a bezpečnostní složky. To ukázalo poměrně výraznou otevřenost britského modelu k přímému zapojení GCHQ, na rozdíl od amerického modelu, kde NSA není přímo angažovaná do případů, které se týkají vlastníků anebo provozovatelů kritické infrastruktury.[48]

V roce 2007 bylo NISCC začleněno do Centra pro ochranu národní infrastruktury (CPNI), které se stalo součástí britské zpravodajské organizace MI5. CPNI se nadále zaměřovalo spíše na sdílení poradenství a informací důležitých pro obranu než na operativní úlohu. V té době si již někteří vysocí úředníci uvědomovali potřebu ambicióznějšího a

[47] "Cabinet Office and The Rt Hon Lord Maude of Horsham, 'Government launches information sharing partnership on cyber security,' GOV.UK, 27. 3. 2013, https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security (staženo 8. 10. 2023).
[48] Chris Ensor, "GCHQ, the National Technical Authority for Information Assurance," Government security blog, 11. 8. 2014, https://securityprofession.blog.gov.uk/2014/08/11/gchq-the-national-technical-authority-for-information-assurance/ (staženo 8. 10. 2023).

organizovanějšího úsilí v oblasti kybernetické bezpečnosti. Vláda se již dříve v omezené míře věnovala národnímu strategickému plánování, a to prostřednictvím zveřejnění Národních strategií zajištění bezpečnosti informací v letech 2003 a 2007. Tyto dokumenty však postrádaly prvky komplexní národní strategie se strategickými prioritami a dostatečným finančním rozpočtem.[49]

V roce 2009 došlo k vypracování první skutečné strategie kybernetické bezpečnosti ve Spojeném království, známé jako Strategie 2009. Tato strategie schválila několik opatření, včetně zvýšení vládního financování technologií souvisejících s kybernetickou bezpečností a úsilí o rozšíření počtu zaměstnanců s kybernetickým vzděláním. Tato strategie také obsahovala dvě významné organizační reformy, které měly dále posílit opatření v oblasti kybernetické bezpečnosti.[50]

Strategie z roku 2009 zavedla vytvoření meziresortního operačního střediska kybernetické bezpečnosti, jehož hostitelem je CESG GCHQ. Toto operační středisko plnilo několik úkolů, včetně koordinace zpravodajských informací, aby mohlo lépe komunikovat kybernetické hrozby vládě. Jeho cílem bylo také sdílet zpravodajské informace o hrozbách se širokou veřejností, což navazovalo na práci v oblasti sdílení informací, kterou dříve pro vlastníky/provozovatele kritické národní infrastruktury vykonával CPNI. Kromě toho mělo operační středisko plnit operativní úlohu při koordinaci reakce nkterý sea incidenty v případech, do nichž se GCHQ zapojovala již přinejmenším od výše zmíněného pokusu o vydírání v roce 1995, kdy byly cílem finanční instituce v Londýně. To zdůraznilo flexibilní operační povahu britského modelu ve srovnání s formálnějšími omezeními amerického modelu.[51]

Další organizační reforma obsažena ve strategii z roku 2009 se týkala samotného úřadu vlády. Dříve se otázky kybernetické bezpečnosti řešily ad hoc, chyběly universální

[49]"Centre for the Protection of National Infrastructure (CPNI)", OECD, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/centrefortheprotectionofnationalinfrastructurecpni.htm#:~:text=CPNI%20was%20formed%20on%201,NSAC (staženo 11. 10. 2023).
[50]John Oates, "UK.gov decides best form of cyber defence is attack", The Register, 25. 6. 2009, https://www.theregister.com/2009/06/25/uk_cyber_security_strategy/ (staženo 11. 10. 2023).
[51]"Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space", Cabinet Office, červen 2009, Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space CM 7642 (publishing.service.gov.uk) str. 12, (staženo 11. 10. 2023).

předpisy a jasné rozdělení odpovědnosti. K nápravě tohoto stavu tato strategie určila sedmnáct samostatných "pracovních směrů" a vyzvala ke zřízení nového Úřadu pro kybernetickou bezpečnost v rámci Úřadu vlády, později přejmenovaného na Úřad pro kybernetickou bezpečnost a informační bezpečnost (OCSIA). Úkolem OCSIA bylo sledovat pokrok příslušných agentur při plnění pracovních směrů a podporovat koordinaci mezi jednotlivými resorty.[52]

V roce 2011 byl vydán nový dokument nazvaný Strategie kybernetické bezpečnosti Spojeného království, který nahradil strategii z roku 2009. Tyto dokumenty se shodovaly co do cílů, kterých chtěly dosáhnout, avšak strategie z roku 2011 obsahovala podstatně silnější rétoriku ohledně nebezpečnosti kybernetických hrozeb a zdůrazňovala naléhavou potřebu přijmout účinná opatření. Strategie z roku 2011 zahrnovala zejména závazek investovat přibližně 860 milionů liber během pětiletého období, známého jako Národní program kybernetické bezpečnosti.[53]

Dokument rovněž zdůrazňuje potřebu sdílení informací mezi jednotlivými resorty. V roce 2013 GCHQ se ve spolupráci s MI5 a Národní kriminální agenturou vytvořil vládní subjekt Cyber Security Information Sharing Partnership (CiSP), jehož cílem je usnadnit výměnu zpravodajských informací o kybernetických hrozbách v reálném čase. Na rozdíl od předchozích modelů bylo CiSP navrženo tak, aby zahrnovalo různá odvětví, a ne aby se týkalo jen konkrétního sektoru. Do roku 2015 se prostředí digitální spolupráce CiSP účastnily stovky organizací ze soukromého sektoru a tisíce jednotlivců, přičemž jeho dosah se postupem času dále rozšiřoval.[54]

GCHQ ve spolupráci s britskými telekomunikačními společnostmi podpořila přijetí systémů pro automatickou detekci známých indikátorů kompromitace (IOC). Tento přístup, známý jako "aktivní obrana", představoval odklon od pasivnějších obranných

[52] "Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space", Cabinet Office, červen 2009, Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space CM 7642 (publishing.service.gov.uk) str. 12, (staženo 11. 10. 2023).
[53] "Cabinet Office and National Security and Intelligence, 'The UK Cyber Security Strategy 2011-2016: Annual Report,' 14. 4. 2016, https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report (staženo 20. 10. 2023).
[54] "Francis Maude, 'Cyber Security Information Sharing Programme,' GOV.UK, 27. 3. 2013, https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme (staženo 20. 10. 2023).

strategií a stal se běžným termínem v kruzích britské politiky kybernetické bezpečnosti.

Mezi institucionální inovace v tomto období patřilo zřízení britského týmu pro reakci na počítačové hrozby (CERT). CERT na národní úrovni byl klíčovým cílem uvedeným ve strategii z roku 2011, který měl řešit potřebu jednoho společného kontaktního místa a hlavního koordinátora v případě závažných kybernetických incidentů. Bylo účelné začlenit Partnerství pro sdílení informací o kybernetické bezpečnosti (CiSP) do CERT. Kromě toho bylo v roce 2013 zřízeno Centrum pro vyhodnocování kybernetických rizik (CCA) jako fúzní centrum pro analýzu všech zdrojů kybernetických hrozeb a incidentů. Po vzoru již existujícího podobného centra pro boj proti terorismu bylo CCA umístěno v rámci GCHQ.[55]

Přestože přijetím těchto strategií bylo dosaženo významného pokroku, bylo jasné, že i přes přijatá opatření se dopady škodlivých kybernetických aktivit zvyšují. Někdejší vedoucí Úřadu pro kybernetickou bezpečnost a informační zabezpečení (OCSIA) se tedy inspiroval izraelskou organizací pro kybernetickou bezpečnost a uvažoval, zda by se nedalo udělat více v této oblasti pro Spojené království. Vláda se tehdy zaměřila především na sdílení informací ve větším rozsahu a dobrovolné programy, které měly přispět ke zlepšení obrany soukromého sektoru, avšak rozhodnutí o investicích do kybernetické bezpečnosti ponechala každému subjektu k úvaze. Bylo však zřejmé, že tento přístup nepřináší dostatečně rychlé zlepšení. Vláda začala uvažovat o přímější roli při posilování obrany soukromého sektoru.[56]

Další změny nastaly za administrativy premiéra Camerona, který se rozhodl pro změny v institucích spíše než pro větší zásahy jako je striktní rozdělení odpovědnosti anebo nové právní regulace. To vedlo k vytvoření Národního centra kybernetické bezpečnosti (NCSC). NCSC sloučilo různé vládní instituce a funkce v oblasti kybernetické bezpečnosti pod jeden, dobře strukturovaný a veřejnosti přístupný subjekt. Jeho cílem bylo zajistit soulad,

[55] "Cabinet Office and The Rt Hon Lord Maude of Horsham", 'UK launches first national CERT,' GOV.UK, 31.3. 2014, https://www.gov.uk/government/news/uk-launches-first-national-cert (staženo 20. 10. 2023).
[56] Stuart Littlewood, "Look Who's in Charge of UK Government Cyber Security," Global Research, 8. 11. 2015, https://www.globalresearch.ca/look-whos-in-charge-of-uk-government-cyber-security/5487359 (staženo 25. 10. 2023).

řešit problémy s koordinací a vybudovat si jméno, kterému budou lidé věřit.[57]

Do NCSC byly začleněny organizace jako CERT (a systém sdílení informací CiSP), fúzní centrum pro analýzu kybernetického zpravodajství a jiné specifické aspekty kybernetické bezpečnosti. Důležité bylo také zvážit, jak bude oficiálně NCSC umístěn, co do jeho hierarchického postavení. Hlavní možnosti, které připadaly v úvahu, byly, že bude buďto fungovat jako nezávislá vládní agentura, nebo bude existovat jako jeden ze článků, zajišťující meziresortní koordinaci. Také by mohl zaštiťovat již stávající agentury, kterým by se jejich místo v organizační struktuře nezměnilo, podobně, jako americký Úřad ředitele národních zpravodajských služeb. Další možností bylo, že by mohl být začleněn do větší stávající organizace, což je cesta, kterou se vydaly Spojené státy, když v rámci DHS vytvořily CISA. Nakonec bylo rozhodnuto, že NCSC bude součástí GCHQ.
Při zahájení činnosti NCSC byly nastíněny klíčové prvky nového plánu kybernetické bezpečnosti. Tento plán zahrnoval navýšení zdrojů pro vyšetřování kybernetické kriminality a obranu vládních systémů. Důležité bylo, že zahrnoval konsolidaci stávajících obranných funkcí a zavedení nových prostřednictvím vytvoření NCSC.

Tento hybridní přístup byl obecně považován za poměrně inovativní, jelikož zdůrazňoval, že je důležité, aby odpovědnost za to, že bude dobře zajištěna kybernetická bezpečnost nesla příslušná zpravodajská služba. Tento rozdíl mezi modelem NCSC a americkým modelem CISA, kde je první z nich integrován do zpravodajské agentury, jako je GCHQ, a nikoli oddělen jako NSA, odráží rozdílné přijetí a akceptaci zpravodajských agentur v příslušných společnostech.

Britský soukromý sektor veskrze ocenil skutečnost, že NCSC byla zařazena do oficiálních složek vlády, které se zabývají kybernetickou problematikou. Byla zde však obava v rámci GCHQ , jelikož jedním z jejích poslání byla i interakce s veřejností a její informovanost o stávající kybernetické situaci státu, což ne všichni považovali za vhodné. Umístění NCSC v rámci GCHQ nicméně podporovala řada argumentů, včetně odborných znalostí GCHQ v oblasti kybernetické bezpečnosti.

[57]Robert Hannigan, "Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre," Royal United Services Institute, 27. 2. 2019, https://www.rusi.org/explore-our-research/publications/occasional-papers/organising-government-cyber-creation-uks-national-cyber-security-centre (staženo 25. 10. 2023).

Pravomoci, které mají NCSC a CISA jsou v obou státech velmi podobné. Zahrnují vládní systémy, soukromou kritickou infrastrukturu, ale i poskytování služeb na podporu bezpečnosti, jako je posuzování zranitelnosti a technické poradenství. Je však třeba upozornit na důležité rozdíly mezi NCSC a CISA. NCSC hraje ve srovnání s CISA větší roli při koordinaci reakcí na závažné kybernetické incidenty, zejména v souvislosti se zřízením funkce Národní bezpečnostní rady a vytvořením nového úřadu národního kybernetického ředitele ve Spojených státech. Britský přístup s umístěním NCSC v rámci GCHQ je popisován jako jednotnější a propojenější s odbornými znalostmi největší a nejschopnější instituce a zároveň těží z flexibility britského politického systému ve vztahu ke zpravodajským službám.

Za zmínku stojí i rozvoj kybernetických schopností Spojeného království a vytvoření partnerství mezi ministerstvem obrany a Vládní komunikační centrálou (GCHQ) známého jako Národní ofenzivní kybernetický program. Národní ofenzivní kybernetický program měl za cíl především podpořit spolupráci mezi ministerstvem obrany a GCHQ s cílem zajistit pro Spojené království kybernetické informace světové úrovně. Toto partnerství umožnilo operacionalizaci britských kybernetických kapacit, podobně jako USCYBERCOM zasáhl proti Islámského státu prostřednictvím operace Glowing Symphony.[58]

GCHQ ve spolupráci s ministerstvem obrany v roce 2016 vedla řadu kybernetických operací proti Islámskému státu. Později vyšlo na světlo, že tyto operace zahrnovaly jak narušení, tak manipulaci online komunikace Islámského státu, což účinně zhoršilo jejich operace a propagandu. Kromě toho GCHQ narušila kontrolu Islámského státu nad bezpilotními letouny a manipulovala s komunikací prostřednictvím mobilních telefonů a notebooků, přičemž občas mystifikovala bojovníky Islámského státu zasíláním falešných rozkazů.[59]

[58] Conrad Prince CB, "On the Offensive: The UK's New Cyber Force," Royal United Services Institute, 23. 11. 2020, https://www.rusi.org/explore-our-research/publications/commentary/offensive-uks-new-cyber-force (staženo 25. 10. 2023).
[59] "The Rt Hon George Osborne, 'Chancellor's speech to GCHQ on cyber security", GOV.UK, 17. 11. 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security (staženo 25. 10. 2023).

Tato spolupráce NOCP mezi GCHQ a ministerstva obrany byla pouhým začátkem této spolupráce. Po počátečním úspěchu začaly probíhat plány na vytvoření formálnější institucionální struktury. Pro začátek bylo hlavním návrhem vytvoření dvoutisícové pracovní skupiny složené z pracovníků GCHQ a ministerstva obrany a probíhaly rozsáhlé debaty o tom, zda by nový subjekt vedl pracovník GCHQ, vojenský důstojník nebo dokonce oba.[60]

V roce 2019 bylo oznámeno, že toto nové strategické partnerství mezi GCHQ a ministerstvem obrany bude ukotveno v jednotné instituci s názvem National Cyber Force (NCF). Zatímco zpočátku NCF tvořilo asi tři sta specializovaných pracovníků, v příštích deseti letech se plánuje jejich rozšíření na tři tisíce. Vedle GCHQ a ministerstva obrany se na NCF podílela také britská tajná zpravodajská služba (MI6). Co se týče vedení, tak v čele NCF stojí bývalý pracovník GCHQ, ačkoli tato pozice se může v budoucnu změnit.[61]

Zřízení Národních kybernetických sil (NCF) ve Spojeném království byl jeden z nejdůležitějších kroků, jakými se Spojené království rozhodlo řešit kybernetické hrozby a přizpůsobovat se v kybernetické oblasti. Tento krok spojil zpravodajské služby za účelem boje proti terorismu, organizovanému zločinu a nepřátelským státním aktivitám v kyberprostoru.

2.3 Srovnání strategií kybernetické bezpečnosti Spojených států a Spojeného království

Jak americký, tak britský model v určité míře regulují soukromý sektor, včetně kritické národní infrastruktury. Ve Spojeném království však došlo v poslední době ke změně v souvislosti s implementací směrnice o síťových a informačních systémech a nařízení o bezpečnosti sítí a informací, jejichž cílem je iniciovat změny v připravenosti soukromých subjektů na kybernetické hrozby. Změny v telekomunikačním sektoru přináší také návrh zákona o telekomunikacích, který zavede specifické bezpečnostní požadavky a umožní regulačním orgánům ukládat pokuty.[62]

[60] "Permanent location of National Cyber Force campus announced," GOV.UK, 3. 10. 2021, naposledy upraveno 4. 10. 2021, https://www.gov.uk/government/news/permanent-location-of-national-cyber-force-campus-announced (staženo 25. 10. 2023).
[61] Ibidem.
[62] "Telecommunications (Security) Bill," GOV.UK, naposledy upraveno 15. 1. 2021, https://www.gov.uk/government/collections/telecommunications-security-bill (staženo 29. 10. 2023).

Kybernetická oblast také představuje pro vlády příležitost k realizaci různých politických cílů, včetně vymáhaní práva, špionáže, prevenci ozbrojených konfliktů a odhalování tajných akcí. Kybernetická oblast nijak dramaticky nezměnila povahu špionáže, ale rozšířila se právě i o tuto oblast. Jak Spojené státy, tak Spojené království disponovaly prvotřídními zpravodajskými službami s odbornými znalostmi v oblasti elektronického zpravodajství již dlouho před nástupem rozsáhlé digitalizace. Dá se předpokládat, že Národní bezpečnostní agentura (NSA) v USA a Vládní komunikační ústředna (GCHQ) ve Spojeném království budou hlavními agenturami pro provádění hackerských útoků pro špionážní účely.[63]

V USA nevedl nárůst počtu hackerských útoků za účelem špionáže ke konkrétním legislativním změnám. Právní rámec pro špionáž, zejména v oblasti signálního zpravodajství (SIGINT), se sice v posledních dvou desetiletích poměrně upravoval, díky změnám zákona o dohledu nad zahraničním zpravodajstvím (FISA), tyto změny však nebyly specificky zaměřeny na hacking. Vytvoření systému Section 702 v rámci zákona FISA umožnilo vládě USA vynutit si spolupráci společností podléhajících jurisdikci USA při přístupu ke komunikaci konkrétních osob nacházejících se mimo území Spojených států. Neexistují však žádné zákony, které by se snažily regulovat možnost NSA provádět hackerské útoky mimo území USA za účelem špionáže.[64]

Situace ve Spojeném království je poněkud odlišná. V reakci na rozhodnutí Evropského soudu pro lidská práva (ESLP) z počátku 90. let přijala Velká Británie zákon o zpravodajských službách z roku 1994 (ISA), který stanovil, že všechny tajné zpravodajské služby, včetně GCHQ, fungují s výslovným souhlasem parlamentu. ISA výslovně

"Telecommunications (Security) Act 2021," legislation.gov.uk, 17. 11. 2021, https://www.legislation.gov.uk/ukpga/2021/31/enacted (staženo 29. 10. 2023).

[63] Jack Freund, "Understanding the Distinction Between Cyberwar and Espionage," ISACA, 27. 4. 2022, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-17/understanding-the-distinction-between-cyberwar-and-espionage (staženo 29. 10. 2023).
Jadyn Marks, "Gabbard's Espionage Act Reform Bill Highlights U.S. Government's Recent Responses to National Security Whistleblowers," American Bar Association, 31. 1. 2021, https://www.americanbar.org/groups/crsj/publications/crsj-featured-articles/espionage-act-reform-bill/ (staženo 29. 10. 2023).

[64] Federal Bureau of Investigation, "Foreign Intelligence Surveillance Act (FISA) and Section 702," FBI, https://www.fbi.gov/investigate/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702 (staženo 3. 11. 2023).

zmiňoval zásahy do zařízení spojené s elektronickou komunikací, což je dnes široce chápáno jako hackerství.

Od roku 2016 se hacking v rámci kategorie zasahování do zařízení řídí zákonem o vyšetřovacích pravomocích (Investigatory Powers Act, IPA). IPA zmocňuje státního tajemníka k vydávání příkazů pro GCHQ k provádění hackerských činností, přičemž dohled nad nimi vykonává nezávislý soudní komisař. Proces vydávání příkazů je povinný, pokud existuje jakékoli spojení se Spojeným královstvím, ale je nepovinný, pokud je vyžadována spolupráce s třetí stranou, např. telekomunikační společností.[65]

Významnější změny v USA i ve Spojeném království můžeme pozorovat v institucionálním ukotvení organizací, které mají pokrývat specifika hackingu jako formy špionáže. Obě země vyvinuly nové mechanismy, jak se s tímto vyvíjejícím se prostředím vypořádat. Tradiční nástroje, používané v signálovém zpravodajství (SIGINT), jako je například anténový odposlech, poměrně dlouhou dobu nevyvolávaly obavy ohledně zranitelnosti systémů, co do zabezpečení samotného přenosu. Při zachycení komunikace šlo hlavně o fyzickou blízkost a prolomení šifrování. Navíc systémy, které byly cílem útoku, obvykle nebyly systémy používané vládami USA a Spojeného království anebo širokou veřejností.

Naproti tomu u hackerských útoků vyvstává zásadní otázka, zda je v národním zájmu odhalovat a napravovat zranitelná místa namísto jejich zneužívání ke špionáži. K řešení této otázky zavedly Spojené státy i Velká Británie meziagenturní program nazvaný Proces rovnosti zranitelností (VEP). Tato iniciativa systematicky zvažuje účely, za kterými jsou shromažďovány zpravodajské informace, a oproti jiným iniciativám zahrnuje vstupy subjektů mimo zpravodajskou komunitu. V obou zemích jde v této oblasti o pilotní programy, lze tedy očekávat, že pravděpodobně v blízké době dojde k dalšímu vývoji v této oblasti.[66]

[65] "Intelligence Services Act 1994," legislation.gov.uk, https://www.legislation.gov.uk/ukpga/1994/13/contents (staženo 3. 11. 2023).
[66] "Everything You Know About the Vulnerability Equities Process Is Wrong," Lawfare, https://www.lawfaremedia.org/article/everything-you-know-about-vulnerability-equities-process-wrong (staženo 3. 11. 2023).

Zpravodajské služby nejsou jedinými aktéry, kteří se starají o zachování bezpečnosti v kyberprostoru. Schopnost v případě potřeby účinně provést hackerský útok je stále důležitější pro různé vládní účely, zejména v ozbrojených konfliktech. Moderní armády jsou v mnoha svých aktivitách závislé na počítačových technologiích a kybernetická bezpečnost hraje při ochraně vojenských systémů zásadní roli. Zároveň se armády snaží rozvíjet i své hackerské schopnosti, aby během ozbrojeného konfliktu pochopily, narušily či případně zničily kybernetické schopnosti protivníka.[67]

Jak Spojené státy, tak Velká Británie rozvíjejí své ofenzivní vojenské kybernetické schopnosti souběžně s těmi obrannými. Existují však rozdíly ve způsobu, jakým obě země k této problematice přistupují.

Pro armádu je v případě ozbrojených konfliktů v dnešní době velmi důležité mít útočné kybernetické schopnosti. Dovednosti, které jsou potřebné pro vedení kybernetické války, se však výrazně liší od tradičního náboru a výcviku vojáků. Z toho vyplývá potřeba odlišných nároků, které armáda má na své uchazeče, aby budoucí vojáci skutečně byli schopní kybernetického boje. Sofistikované hackerské operace navíc vyžadují nákladné vzdělávání vojáků a často naráží na omezenou výpočetní infrastrukturu, kterou armády obvykle v této oblasti disponují.[68]

Jak už bylo zmíněno v předchozím textu, Spojené státy i Velká Británie reagovaly na kybernetické hrozby světové úrovně zřízením Národní bezpečnostní agentury (NSA) a Vládního komunikačního ústředí (GCHQ). Obě země však zvolily odlišné přístupy, co se týče jejich institucionálního ukotvení z hlediska hierarchie a jejich pravomocí. Ve Spojených státech byl zvolen inkubační model. Spojené státy zřídily USCYBERCOM jako samostatnou vojenskou organizaci, ale začlenily ji vedle NSA ve Fort Meade. Toto uspořádání zahrnovalo společný sdílený personál a vytvořilo infrastrukturu s dvojím vedením. Ačkoli se očekávalo, že se USCYBERCOM nakonec od NSA oddělí, jeho oddělení se neustále odkládalo. V současnosti právní předpisy přijaté Kongresem brání

[67] James A. Lewis, "Cyber Security and the Intelligence Community," Belfer Center for Science and International Affairs, naposledy upraveno 15. 12. 2021, https://www.belfercenter.org/publication/cyber-security-and-intelligence-community (staženo 5. 11. 2023).
[68] James Andrew Lewis, "The Rationale for Offensive Cyber Capabilities," Strategic Technologies Blog, CSIS, naposledy upraveno 13. 7. 2021, https://www.csis.org/blogs/strategic-technologies-blog/rationale-offensive-cyber-capabilities (staženo 5. 11. 2023).

formálnímu oddělení, dokud nebudou splněna určitá kritéria, která jsou momentálně stále v nedohlednu.[69]

Mnozí považují americký model za atraktivní hybrid, který poskytuje vysokou úroveň co do jejích kompetencí a ukazuje se jako poměrně účinný. Mnozí také tvrdí, že toto uspořádání rovněž vytváří kreativnější prostředí, které pomáhá při narušování systému protivníka.
Jak americká Národní bezpečnostní agentura (NSA), tak britská Vládní komunikační centrála (GCHQ) jsou styčnými organizacemi pro sběr informací SIGINT a nejdůležitějšími organizacemi pro zajišťování informací. Role NSA a GCHQ se však výrazně liší. Zatímco NSA je v USA vyloučena z operačního zapojení do ochrany civilních vládních a soukromých systémů, GCHQ má ve Spojeném království daleko pružnější přístup. Rozdíly mezi systémy USA a Spojeného království jsou ovlivněny různými faktory. Například obavy veřejnosti z činnost NSA v USA jsou výraznější než obavy z GCHQ ve Spojeném království. Z politického hlediska je náročnější rozšířit pravomoci NSA, právě z důvodu obav z nesouhlasu veřejnosti.

Narozdíl od Spojených států nerozlišuje Spojené království, co se terminologie týče, mezi tajnými akcemi a speciálními vojenskými operacemi. Právě tato dvojznačnost umožňuje pružněji a pohotověji reagovat na rychle se měnící hrozby bez zbytečných byrokratických omezení. NCF působí v kompetenci ministrů obrany i zahraničí, ačkoli z veřejných záznamů není jasné, kdy konkrétně je k určitým operacím zapotřebí jejich souhlas.[70]
Spojené státy i Spojené království si kladou za cíl potírat také škodlivé kybernetické aktivity, ke kterým dochází mimo ozbrojený konflikt. Patří sem činnosti, které způsobují škody v samotné kybernetické oblasti jako takové, i ty, které se spoléhají na kybernetickou oblast jako na prostředek pro způsobení nekybernetických škod.

V reakci na to byly vyvinuty snahy o posílení kybernetické obrany a uvalení persekucí na útočníky prostřednictvím sankcí či trestního stíhání. Ke zlepšení této obrany však dochází

[69] Ronda Swaney, "Why Keep Cybercom and NSA's Dual-Hat Arrangement?," Security Intelligence, 11. 9. 2023, https://securityintelligence.com/articles/why-keep-cybercom-and-nsas-dual-hat-arrangement/ (staženo 6. 11. 2023).
[70] "Responsible Cyber Power in Practice," GOV.UK, 4. 4. 2023, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html (staženo 6. 11. 2023).

podstatně pomaleji než v oblasti vojenské a sankce, jimiž se státy snaží pachatele potrestat, nemusí pachatele vždy úspěšně zasáhnout. Obě země proto obrátily svou pozornost k využití kybernetických prostředků k potření těchto škodlivých aktivit přímo u jejich zdroje.[71]

Úkoly USCYBERCOM a NCF nejsou zaměřeny pouze na kybernetický boj jako takový. Zahrnují také operace, které jsou svou povahou spíše preventivní. Cílem těchto operací je narušit sítě protivníka a zastavit nebo zabránit škodlivé činnosti dříve, než stačí napáchat v jejich systému jakoukoli škodu. Toto avšak vyvolává důležité otázky ohledně institucionálního uspořádání a právního rámce, který se v takových případech dá aplikovat. Plně hybridní přístup Spojeného království prostřednictvím NOCP a nyní již i NCF relativně usnadnil řešení institucionálních otázek souvisejících s těmito nebojovými misemi. NCF již při svém založená měl za úkol klást důraz i na tyto mise.[72]

Příkladem takové mise může být například potírání dezinformací s cílem jejich co nejmenšího rozšíření mezi své občany. Úloha NCF v reakci na dezinformační kampaně a falešné zprávy zahrnuje nabourávání zahraničních systémů za účelem odstranění falešných informací přímo z jejich zdrojů. Zabývá se také jinými problémy, které mají vysokou společenskou škodlivost, jako je zneužívání dětí online a organizovaná kybernetická kriminalita.[73]

I když se výše zmíněné aktivity nedají přesně zařadit do tradičních kategorií kybernetických hrozeb, mají společnou charakteristiku - pocházejí obvykle z různých lokalit, povětšinou v zahraničí, což je daleko hůře postižitelné než aktivity, které se dějí na území státu. Avšak právě proto je díky své flexibilitě NCF přesně tou institucí, která by

---

[71] "Government-led Initiatives as Critical to National Cyber Defenses," TechHQ, 19. 4. 2022, https://techhq.com/2022/04/government-led-initiatives-as-critical-to-national-cyber-defenses/ (staženo 7. 11. 2023).

[72] "CYBER 101 - Defend Forward and Persistent Engagement," U.S. Cyber Command, 25. 10. 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/ (staženo 7. 11. 2023).
"Responsible Cyber Power in Practice," GOV.UK, 4. 4. 2023, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html (staženo 7. 11. 2023).

[73] Bill Goodwin, "National Cyber Force carrying out daily hacking operations to disrupt hostile threats," Computer Weekly, 4. 4. 2023, https://www.computerweekly.com/news/365534733/National-Cyber-Force-carrying-out-daily-hacking-operations-to-disrupt-hostile-threats (staženo 7. 11. 2023).

měla tuto problematiku řešit. Narozdíl od Spojených států, model NCF ve Spojeném království má daleko flexibilnější přístup, což mu umožňuje větší pružnost při řešení těchto nekonvenčních hrozeb bez přílišných obav ohledně překročení jeho institucionálních kompetencí. Právě tato skutečnost ale také vyvolává obavy ohledně zapojení NCF do této problematiky z hlediska možného překročení etických a právních norem.[74]

Můžeme však pokládat za krajně nepravděpodobné, že by NCF aktivně zahajovalo škodlivé kybernetické operace jakožto agresor. Pojmy útok a útočný sice mohou být v tomto ohledu zavádějící, ale pravděpodobnější je, že NCF využívá kybernetické prostředky k narušení škodlivých aktivit, které jsou iniciovaný protivníky. Hlavní úkoly NCF zahrnují především útočné akce v užším slova smyslu, které obvykle spočívají v provádění hackerských útoků za účelem narušení bezpečnosti systému protivníka. Tyto akce však mají i obranný charakter, kdy je jejich cílem zabránit někomu jinému v pokračování způsobování škod. Výše zmíněné příklady uvedené pro NCF odpovídají tomuto defenzivnímu využití hackingu.[75]

Také můžeme nalézt podobnosti mezi NCF a modelem preventivních útoků, který přijal USCYBERCOM. Oba tyto instituty čelí různým druhům kybernetických hrozeb a uvědomují si značné přínosy, jež přináší toto preventivní narušování sítí protivníka, přímo na jeho serverech. Koncepce USCYBERCOM pro preventivní útok zahrnuje obranné operace v sítích spojenců, jakož i provádění operací v takzvaném červeném kyberprostoru s cílem narušit škodlivou kybernetickou činnost přímo u jejího zdroje v zahraničí. Pojem červený kyberprostor označuje části kyberprostoru, které vlastní nebo ovládá protivník nebo nepřítel. V tomto případě ovládat znamená více než jen pouhou jeho přítomnost, protože hrozby mohou mít zastřený přístup k nějaké z částí globálního kyberprostoru, kde je jejich přítomnost prozatím nezjištěna. V tomto případě kontrolovaný znamená schopnost řídit operace určitého článku nebo uzlu v kyberprostoru s vyloučením ostatních hráčů, kteří by se chtěli na řízní podílet. Mezi oběma přístupy však existují určité rozdíly. Narozdíl od

[74] Danny Steed, "Evaluating the National Cyber Force's 'Responsible Cyber Power in Practice'," Royal United Services Institute, 9. 2. 2021, https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice (staženo 10. 11. 2023).
[75] Danny Steed, "The National Cyber Force: directions and implications for the UK," Elcano Royal Institute, 9. 2. 2021, https://www.realinstitutoelcano.org/en/analyses/the-national-cyber-force-directions-and-implications-for-the-uk/ (staženo 10. 11. 2023).

NCF má USCYBERCOM také své stálé obranné povinnosti pro systémy přímo americké armády. Americký model je proto opět spíš hybridní, což v některých případech vede k neshodám, co se týče jeho kompetencí.[76]

USCYBERCOM zpočátku čelil námitkám týkajícím se jeho pravomoci provádět kybernetické operace v zahraničí mimo ozbrojený konflikt a možného zařazení jeho operací do kategorie tajných akcí v rámci dohledu spojeného se CIA. Tyto námitky vyvolaly otázky, zda by USCYBERCOM měl takové operace vůbec provádět, nebo zda by měl podléhat systému dohledu nad tajnými akcemi, včetně potřeby písemných prezidentských povolení.[77]

Tyto námitky týkající se pravomoci USCYBERCOM provádět operace mimo síť řešil Kongres v průběhu let prostřednictvím změn zákonů. V současné době má USCYBERCOM jasnou pravomoc provádět takové operace, zejména proti Rusku, Číně, Íránu a Severní Koreji, neboť Kongres mu za podmínky splnění určitých podmínek udělil výslovné oprávnění. Pokud však u dané operace nejde o tyto státy, právní situace se komplikuje, protože chybí konkrétní zákonné zmocnění pro takovou misi. V takových případech může oprávnění provádět operace mimo síť stále existovat na základě obecných pravidel platných při sebeobraně státu, které jsou dány ústavou a dalšími obecně platnými zákony. Přesto je pro USCYBERCOM pravděpodobně obtížnější než pro NCF ve Spojeném království zapojit se do operací na narušení bezpečnosti zahrnujících nestátní subjekty zapojené do trestné činnosti. Nedávné zprávy však naznačují, že modely USA a Spojeného království se v tomto ohledu pravděpodobně budou v praxi sbližovat, jak jsme

[76] Erica D. Lonergan, "Defend Forward: Adapting Offense and Defense Strategy to Cyberspace," Yale Cyber Leadership Forum, 20. 6. 2021, https://www.cyber.forum.yale.edu/blog/2021/7/20/defend-forward-adapting-offense-and-defense-strategy-to-cyberspace (staženo 10. 11. 2023).
Tim Stevens, Rory Cormac, Erica D Lonergan, Dan Lomas, Dr. Pia Hüsch, and Joe Devanny, "Evaluating the National Cyber Force's 'Responsible Cyber Power in Practice'," Royal United Services Institute, 14. 4. 2023, https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice (staženo 10. 11. 2023).
Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," Lawfare, 28. 5. 2019, https://www.lawfaremedia.org/article/cyber-commands-strategy-risks-friction-allies (staženo 10. 11. 2023).
[77] Mark Pomerleau, "New authorities mean lots of new missions at Cyber Command," C4ISRNET, 8. 5. 2019, https://www.c4isrnet.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/ (staženo 13. 11. 2023).
Michael Martelle, ed., "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY," National Security Archive, 21. 1. 2020, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony (staženo 13. 11. 2023).

mohli pozorovat na operaci USCYBERCOM zaměřenou na síť TrickBot.[78]

Srovnání můžeme provést také s mezinárodním právním rámcem upravujícím útočné operace mimo ozbrojený konflikt. Spojené státy i Spojené království uznávají, že mezinárodní právo zakazuje použití síly a donucovací zásahy. Avšak existují rozdíly v názorech na to, zda vůbec existuje pravidlo mezinárodního práva, které výslovně zakazuje zásahy do suverenity jiných států, které by byly pod hranicí donucovací intervence, jako například určité operace v kyberprostoru. Ačkoli vlády USA a Spojeného království v současné době sdílejí v této otázce podobný názor, spekuluje se o možnosti změny a vytvoření nových pravidel, která by byla terminologicky přesnější.[79]

Za zmínku také stojí rozdíly ve vnímání státní suverenity mezi těmito státy. Postoj Spojeného království k otázce suverenity je jasný, kdy uznává její význam jako jeden ze základních principů v mezinárodním systému. Avšak výslovně neříká, že by suverenita sama o sobě představovala samostatné pravidlo mezinárodního práva. Někteří sice prosazují, aby bylo jasně definováno specifické pravidlo porušení územní suverenity i v kybernetickém prostoru, týkající se zasahování do počítačových sítí jiného státu bez jeho souhlasu, doposud se tomu však tak nestalo. Vláda Spojeného království tedy i v oficiálních dokumentech zastává názor, že v současném mezinárodním právu neexistuje žádné konkrétní pravidlo, které by zakazovalo nekonsensuální kybernetické operace jako porušení svrchovanosti. Právě tento postoj, v kombinaci s institucionálními pravomocemi, které má spojení GCHQ, ministerstva obrany a MI6 do Národní kybernetické síly (NCF) umožňuje NCF potenciálně podnikat kroky proti systémům fyzicky umístěným v jiných zemích bez jejich souhlasu.[80]

Naproti tomu postoj vlády USA k otázce suverenity není tak jednoznačný, jako je tomu v případě Spojeného království. Spojené státy zastávají názor, že nekonsensuální kybernetické operace na území jiného státu automaticky neporušují mezinárodní právo,

[78] Mark Pomerleau, "New authorities mean lots of new missions at Cyber Command," C4ISRNet, 8. 5. 2019, https://www.c4isrnet.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/ (staženo 13. 11. 2023).
[79] Harriet Moynihan, "The Application of Sovereignty in Cyberspace," Chatham House, 2. 12. 2019, https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace (staženo 15. 11. 2023).
[80] Ibidem.

nicméně připustil, že přesná hranice, kdy by takové operace porušovaly suverenitu, se stále zkoumá a bude spíše stanovena praxí a právními obyčeji států. Někteří zastánci prosazují mezinárodní pravidlo svrchovanosti a naznačují, že některé kybernetické operace bez souhlasu porušují suverenitu státu.[81]

Tato oblast mezinárodního práva, zejména pokud jde o kybernetické operace je stále značně zavádějící. I Tallinský manuál, který pojednává mimo jiné i o aplikaci mezinárodního práva na kybernetickou válku, se tuto otázku snažil vyřešit. Problém spočívá hlavně v tom, v jakých případech lze považovat kybernetikou operaci, zejména takovou, která je vedena z území mimo stát a má za následek škody, újmu nebo narušení na území tohoto státu, za operaci, která porušila suverenitu státu. Budoucí směřování obou zemí v této otázce tedy zůstává nejisté.[82]

Pokud by Spojené státy změnily svůj postoj k této otázce, muselo by se to nutně odrazit i ve změně kompetencí mezi institucemi. V současné době se na operace USCYBERCOM nevztahuje vnitrostátní právní rámec USA, který platí pro tajné operace. Tajné operace prováděné CIA musí být v souladu s ústavou a zákony Spojených států, ale ne nutně s mezinárodním právem. Pokud by USCYBERCOM působil podle pravidla suverenity, mohl by potenciálně čelit omezení svobody svého jednání, neboť ministerstvo obrany obecně musí dodržovat mezinárodní právo.[83]

Podobná změna v této otázce by v případě Spojeného království měla ještě širší důsledky. Narozdíl od USA britský systém postrádá možnost těchto výše zmíněných institucionálních kliček, co do vnitrostátního práva, které by umožňovaly jeho obcházení. To může vysvětlovat, proč ve Spojeném království je kladen tak velký důraz na terminologii a na mezinárodněprávní hranice a proč odmítají uznání suverenity jako pravidla, spíše než jako zásady mezinárodního práva. Změna názoru v otázce suverenity by

[81]Michael Schmitt, "US Transparency Regarding International Law in Cyberspace," Just Security, 15. 11. 2016, https://www.justsecurity.org/34465/transparency-international-law-cyberspace/ (staženo 17. 11. 2023).
[82] Ibidem.
[83] Robert Chesney, "The Domestic Legal Framework for U.S. Military Cyber Operations," Lawfare, 5. 8. 2020, https://www.lawfaremedia.org/article/domestic-legal-framework-us-military-cyber-operations (staženo 17. 11. 2023).

měla dopad nejen na ministerstvo obrany Spojeného království, ale i na celou vládu.[84]

Za zmínku stojí i vývoj hybridního modelu kybernetických operací Spojených států, který je aktuálně považovaný spíš za konečný stav, než jako dočasné řešení, jak tomu bylo původně při jeho vytvoření. Tento model umožňuje ozbrojeným silám využívat kompetence zpravodajských agentur, aniž by to ohrozilo jejich původní poslání. Přístup Spojeného království ukazuje způsob, jak se dá dosáhnout podobného cíle prostřednictvím přímějšího a integrovanějšího přístupu, i když v menším měřítku než tomu je ve Spojených státech.

Na rozdíl od Národní bezpečnostní agentury (NSA) ve Spojených státech není Vládní komunikační ústředna (GCHQ) ve Spojeném království součástí ministerstva obrany. Stejně jako NSA však GCHQ vždy hrálo klíčovou roli při podpoře bojových operací, zejména při shromažďování zpravodajských informací a ochraně vojenských komunikací. Když byl kybernetický prostor uznán za oficiální válečnou sféru, stálo Spojené království před rozhodnutím, jak k této nové výzvě přistoupit.[85]

Britský systém vzhledem ke svému rozsahu neumožňuje kopírovat americký model samostatného kybernetického velitelství vedle NSA, nehledě na to, že by pro Spojené království byl finančně neúnosný. Místo toho se rozhodli pro integrovaný vojensko-civilní model, který by své nové kompetence sladil se stávajícími odbornými znalostmi a kapacitami GCHQ. Tento přístup dával smysl vzhledem k tomu, že GCHQ již disponovala kompetencemi, přístupem a zdroji potřebnými pro ofenzivní kybernetické operace. Kromě toho měla GCHQ pro takové operace zákonné pravomoci a v omezeném počtu případů již útočné kybernetické operace prováděla na základě pověření ministra.

V roce 2014 Spojené království formalizovalo Národní ofenzivní kybernetický program, aby tento integrovaný přístup dále podpořilo a upevnilo. Tento program poskytl rámec pro

[84] United Kingdom Government, "Application of international law to states' conduct in cyberspace: UK statement," 3. 6. 2021, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (staženo 17. 11. 2023).
[85] Jake Harrington and Riley McCabe, "The Case for Cooperation: The Future of the U.S.-UK Intelligence Alliance," CSIS, 15. 3. 2022, https://www.csis.org/analysis/case-cooperation-future-us-uk-intelligence-alliance (staženo 19. 11. 2023).

využití schopností GCHQ na podporu vojenských operací, přičemž těžil z již existující přítomnosti vojenských důstojníků v řadách pracovníků GCHQ. Tento přístup eliminoval potřebu nových právních oprávnění a zefektivnil proces provádění útočných kybernetických operací.[86]

Zkušenosti USA i Spojeného království poukazují na rozdílné přístupy k dosažení cíle, kterým je integrace schopností zpravodajských služeb do vojenských operací v kybernetické oblasti. Zatímco USA zvolily hybridní model se samostatnými subjekty, Spojené království zvolilo integrovanější přístup prostřednictvím GCHQ. Oba modely mají své výhody a ukazují, že pravděpodobně neexistuje univerzální řešení, které by se dalo dobře aplikovat na obě země.

Navzdory společnému právnímu systému, závazku k dodržováním právního státu a dlouhodobé spolupráci ve vojenských a zpravodajských záležitostech se přístupy Spojených států a Spojeného království v oblasti kybernetické bezpečnosti liší. Spojené státy se svými většími zdroji v posledních letech investovalo do rozvoje svých bezpečnostních institucí, zejména USCYBERCOM. Na druhé straně Spojené království neupřednostňuje stejné rozdělení kompetencí a je otevřenější zapojení své zpravodajské agentury GCHQ do činností, které nejsou primárně zpravodajského charakteru. Zatímco v obranných kybernetických přístupech se obě země do značné míry shodují, existují i významné rozdíly, zejména pokud jde o zapojení jejich nejdůležitějších institucí, jako jsou NSA a GCHQ, do aktivit mimo zpravodajské služby. Čas možná ukáže, který model je účinnější, ale je pravděpodobné, že oba přístupy mají své přednosti a slabiny v závislosti na konkrétním kontextu a okolnostech.

3. Kybernetické incidenty a jejich dopady

Tato část práce je věnována nastínění možností, které státy mají, stanou-li se obětmi kybernetického útoku. Práce následně podrobněji představuje reakci obou států na dosud největší kybernetické incidenty, které postihly jak Spojené státy, tak i Spojené království.

[86] Conrad Prince, "On the Offensive: The UK's New Cyber Force," Royal United Services Institute, 23. 11. 2020, https://www.rusi.org/explore-our-research/publications/commentary/offensive-uks-new-cyber-force (staženo 19. 11. 2023).

Těmito incidenty jsou útok ransomwaru WannaCry v roce 2017, malwaru NotPetya rovněž v roce 2017, případ kybernetické špionáže, který proběhl na serveru SolarWinds v roce 2020 a státem sponzorovaný kybernetický útok na servery Microsoft Exchange v roce 2021.

3.1 Možnosti reakcí na kybernetické incidenty

Pakliže dojde k narušení kybernetické bezpečnosti státu, mají vlády řadu nástrojů, kterými mohou na kybernetické zločiny odpovědět. Například to mohou být nástroje ekonomické, jako jsou sankce proti vládním činitelům, jednotlivým aktérům, soukromým organizacím, nebo cestovní omezení pro jednotlivce (uplatňované buď samostatně, nebo ve spolupráci s jinými státy). V úvahu připadají také politická nebo diplomatická opatření, jako je vyhoštění zahraničních vládních úředníků, kontrarozvědné operace, odhalení malwaru nebo taktiky protivníka. V určitých případech může být taková sankce v gesci orgánů činných v trestním řízení - zabavení majetku, soudem nařízená demontáž infrastruktury, zatčení či stíhání.[87]

Ne všechny tyto možnosti budou samozřejmě zvažovány v každém případě kybernetického incidentu, který se týká vládních sítí a systémů Spojených států nebo Spojeného království. Jsou zde uvedeny proto, aby byla nastíněna škála potenciálních možností, které mohou být zvažovány, i když mohou být v daný moment odmítnuty jako příliš eskalační anebo nepřiměřené incidentu. Dostupné možnosti reakce se rovněž netýkají pouze kybernetické oblasti. Nejúčinnější reakce může být někdy právě ta mimo kybernetickou oblast. Žádná reakce je rovněž formou reakce a rovněž může být vzkazem protivníkovi.

V této práci je pomocí konkrétních případů ilustrována především metoda cyber detterence, což můžeme do češtiny volně přeložit, jako metoda odstrašování či odrazování. Odrazování je a vždy bylo součástí společné existence ve společnosti, ať už mezi

[87] Jason Bartlett and Megan Ophel, "Sanctions by the Numbers: Spotlight on Cyber Sanctions," Center for a New American Security, 4. 5. 2021, https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber (staženo 19. 11. 2023).
United States Department of State, "Cybercrime," U.S. Department of State, https://www.state.gov/cybercrime (staženo 19. 11. 2023).
"Practical Issues in Cyber-Related Sanctions," in The Guide to Sanctions, Fourth Edition, Global Investigations Review, 29. 11. 2023, https://globalinvestigationsreview.com/guide/the-guide-sanctions/fourth-edition/article/practical-issues-in-cyber-related-sanctions (staženo 21. 11. 2023).

jednotlivci, skupinami nebo národy. Například zámky nebo alarmy proti vloupání tvoří základní formu odstrašení, jehož cílem je přesvědčit potenciální narušitele, že vloupání do určitého objektu by bylo velmi obtížné. Během studené války se díky ničivé síle jaderných arzenálů obou mocností stala teorie odstrašení ústřední součástí strategie národní bezpečnosti. Ačkoli nelze prokázat, zda tato strategie zabránila další válce, nebo zda by válka stejně nevypukla, svět vyšel ze studené války bez přímé konfrontace mezi oběma bloky.

Vlády Spojených států i Spojeného království se již dlouho snaží účinně odrazovat od kybernetických útoků (nebo je zastavovat) a reagovat na ně tak, aby se jim v budoucnu podařilo zabránit. Oba cíle se ale mohou zdát těžko dosažitelné, protože četnost kybernetických útoků, od těch drobných až po ty nejvýznamnější, se v průběhu času rapidně zvyšuje. Tyto útoky ukazují, že účinného odstrašení je v kyberprostoru obtížné dosáhnout. S kybernetickými útoky jsou spojeny skutečnosti, které se naprosto vymykají dřívějšímu pojetí politiky odstrašování v jiných sférách. Mnozí však stále považují politiku odstrašení za nezbytný krok k udržení bezpečnosti kyberprostoru a odstrašování považují za ústřední myšlenku při tvorbě nových kybernetických strategií.[88]

V březnu 2020 vydal americký Kongres zprávu, v níž se vyslovil pro strategický přístup ke kybernetické bezpečnosti "kybernetického odstrašení v několika vrstvách". Ačkoli Kongres a prezident prosazují politiku odstrašování v kyberprostoru, jejich dosavadní kroky se zaměřují především na odrážení akcí protivníka. Někdy je toto zaměření záměrné - strategie ministerstva obrany "vytrvalého zapojení" usiluje o to, aby protivníky zaměstnala a odepřela jim čas a zdroje k provedení útoků.[89]

Na tomto místě by bylo také vhodné vymezit strategii odstrašování vůči strategii odepření. Strategie odstrašení a odepření v oblasti kybernetické bezpečnosti představují různé

[88]James Andrew Lewis, "Deterrence and Cyber Strategy," CSIS, 15. 11. 2023, https://www.csis.org/analysis/deterrence-and-cyber-strategy (staženo 21. 11. 2023).
Jeremy Hunt, "Deterrence in the Cyber Age," speech delivered at Glasgow University, 7. 3. 2019, UK Government, https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary (staženo 21. 11. 2023).
[89]Cybersecurity: Deterrence Policy, Congressional Research Service, 18. 1. 2022, https://crsreports.congress.gov/product/pdf/R/R47011#:~:text=Generally%2C%20cyberspace%20deterrence%20strategies%20seek,a%20low%20rate%20of%20success str. 1

přístupy k dosažení stejného cíle - bezpečnějšího digitálního prostředí. Tyto strategie se vzájemně nevylučují. Často jsou implementovány současně a jejich kombinace může přijatá opatření značně posílit. Obecně platí, že v případě kybernetické bezpečnosti se strategie odepření snaží zlepšit technologie, procesy a postupy nad věcmi, které máme pod vlastní kontrolou, aby navzdory úsilí protivníka byla úspěšnost útoku nízká. Strategie odrazování se snaží ovlivnit chování jiných osob nebo subjektů - zabránit jim v nežádoucí činnosti.[90]

Definici odepření lze tedy vykládat jako zabránění protivníkovi něco použít. Při tomto výkladu splňuje tuto definici mnoho potenciálních činností v oblasti kybernetické bezpečnosti. Například narušení internetové infrastruktury protivníka brání jeho škodlivému využívání kyberprostoru jako domény a správná konfigurace a údržba vlastních informačních a komunikačních technologií odpírá protivníkovi možnost je využívat. Jedinečnost tohoto výkladu spočívá v tom, že se nezaměřuje na samotné protivníky, ale na věci, které se snaží zneužít. Definici odstrašení lze interpretovat jako ovlivnění protivníka takovým způsobem, který mu zabrání ve škodlivém chování. V tomto modelu se odstrašení opírá o normy a prokázané schopnosti. Jde o nastavování norem na vládní úrovni, především mezi státy a stanovit jasné podmínky co je přijatelné a co ne. Problémem ale je, že pro kyberprostor tyto podmínky teprve vznikají. Konvenční politika odstrašování se opírá o několik podmínek, kdy vývoj a použití určitých útočných schopností je spojeno s vysokými náklady. Tím pádem existuje jen omezený počet aktérů s těmito schopnostmi. Dopustí- li se jakékoli agrese, ví přesně, jaké ponesou následky. Kybernetický prostor se vyznačuje naprosto opačnými podmínkami. Náklady na vstup potenciálních škodlivých aktérů jsou nízké. Existuje jich mnoho (státních i nestátních) a důsledky úspěšných kybernetických útoků jsou pro ně nejednoznačné nebo naprosto neznámé. Z tohoto důvodu se někteří domnívají, že odstrašení v kyberprostoru není v současné době životaschopnou strategií.[91]

Pro úspěšnou aplikaci odstrašovací strategie je důležité zvážit reakce na incidenty v

[90] Robert Morgus, John Costello, Charles Garzoni, a Michael Garcia, "Deterrence by Denial: The Missing Element of U. S. Cyber Strategy," Lawfare, 11. 3. 2020, https://www.lawfaremedia.org/article/deterrence-denial-missing-element-us-cyber-strategy (staženo 21. 11. 2023).
[91] Chris Jaikaran, "Cybersecurity: Deterrence Policy," Congressional Research Service, R47011, 18. 1. 2022, https://www.everycrsreport.com/reports/R47011.html (staženo 23. 11. 2023).

kyberprostoru, které přesahují jeho rámec, jak již bylo nastíněno na začátku této kapitoly. I když odborníci na kybernetickou bezpečnost hrají klíčovou roli při identifikaci faktorů, které je třeba zvážit při zkoumání strategií odstrašování, škála činností, které mají vlády zemí k dispozici k ovlivňování protivníků, je mnohem širší než pouze v oblasti kybernetické bezpečnosti. K zajištění multidisciplinárních řešení účinných strategií odstrašování jsou zapotřebí odborníci napříč obory. Mezi odborníky, s nimiž je třeba zvážit konzultace při přípravě odstrašujících opatření, patří odborníci na konkrétní země, ze kterých často přicházejí kybernetické útoky, jako jsou například Rusko, Čína, Severní Korea anebo Írán. Dále také experti na konkrétní cíle, kterých se v daný moment snažíme docílit, ať už jsou diplomatické, zpravodajské, vojenské nebo ekonomické. Tento postoj zastávají i odborníci na kybernetickou bezpečnost, kteří ač považují kybernetické útoky za výzvu pro počítačovou komunitu, uznávají, ž řešení nemůže být čistě technické. Důležitou strategií, na kterou je vhodné poukázat, je odstrašování pomocí snížení hodnoty kybernetické špionáže pro protivníka. Toho se dá docílit například vytvořením falešné informace a údajů, které se budou jevit jako legitimní, takže protivník buď dojde na základě analýzy k nesprávným závěrům, nebo bude zmaten, co je pravé a co falešné. Aby vláda mohla vést ofensivní kybernetické operace, musí investovat do výzkumu a operačního zabezpečení, které umožňuje opakované použití na utajené akce. To platí zejména pro útoky například na systémy zahraničních vlád. V okamžiku, kdy je útok odhalen, může začít mizet přístup k narušeným systémům, mohou být shromážděny důkazy, které útok přisuzují těm, kdo za ním stojí. Zde je také důležité zdůraznit rozdíl mezi konvenčními zbraněmi a ofensivními kybernetickými schopnostmi. Konvenční zbraně jsou používány v doméně, pro kterou byly vynalezeny. Obrana proti těmto zbraním se často skládá z prostředků uplatňovaných rovněž v té dané doméně. Například balistická střela může být zachycena protiraketovým systémem ve vzduchu dříve, než zasáhne zamýšlený cíl. Útočná kybernetická schopnost však obvykle využívá slabinu v doméně - nebo slabinu proti samotnému systému či síti v kyberprostoru. Obrana proti kybernetickému útoku tak může zahrnovat vývoj a použití nového nástroje nebo opravu stávajícího systému s cílem zmírnit účinek útočného kybernetického nástroje.[92]

[92] Stephanie Pendino, Robert K. Jahn, Sr., a Kirk Pedersen, "U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light," Joint Forces Staff College, 7. 11. 2022, https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/ (staženo 23. 11. 2023).

3.2 Kybernetické incidenty ve Spojených státech a jejich reakce

Spojené státy se z mnoha důvodů potýkají s velmi vysokým počtem kybernetických útoků. Podle zprávy ISACA 2023 State of Cybersecurity (Stav kybernetické bezpečnosti v roce 2023) hlásí 48 % organizací výrazný nárůst kybernetických útoků ve srovnání s předchozími lety. Mezi důvody, proč Spojené státy čelí takovému množství útoků, patří vysoce digitalizovaná infrastruktura, cenné duševní vlastnictví a globální politický a ekonomický vliv, což z nich činí velice atraktivní cíl. Povaha těchto útoků se liší a zahrnuje státem sponzorovanou špionáž, krádeže finančních prostředků zločineckými skupinami i ideologicky motivované hackerské útoky. Tyto hrozby se neustále vyvíjejí a útočníci využívají sofistikované techniky a nová zranitelná místa. To zdůrazňuje nutnost opatření v oblasti kybernetické bezpečnosti a mezinárodní spolupráce při jejich řešení.[93]

K přijetí nutných opatření avšak často dohází až po útocích, které na ně upozorní. Například incident společnosti SolarWinds měl za následek snahu americké vlády posílit svá zranitelná místa ve své kybernetické obraně, kdy Bidenova administrativa, stejně jako jiné administrativy po předchozích kybernetických incidentech, vydala nařízení o prioritách kybernetické bezpečnosti USA. Nařídila federálním ministerstvům a agenturám, aby vypracovaly plány k provozování a obraně svých sítí založené na architektuře nulové důvěry. Je zřejmé, že toto zlepšení kybernetické bezpečnosti amerických vládních systémů bylo nutné, ale bohužel ani to nestačilo k tomu, aby se zabránilo budoucím incidentům. Dosavadní politika Spojených států v kyberprostoru je dostala do situace, kdy se zdráhají uvažovat o určitých reakcích, protože samozřejmě samy provádějí kybernetickou špionáž a proto by pravděpodobně ztratily více omezením sběru kybernetických zpravodajských informací, než by získaly z dohody s Čínou a Ruskem, pokud by se takovou dohodu vůbec podařilo uzavřít a prosadit. Aby však bylo možné vybudovat lepší základ pro reakce USA na kybernetickou špionáž, mělo by mezinárodní společenství vytvořit jasné pokyny pro to, které činnosti jsou v kyberprostoru přijatelné a které nikoli. To by nevyžadovalo, aby se

Mark Spangler, "Offensive Cyber Operations: A National Security Imperative," AFCEA International, 29. 6. 2023, https://www.afcea.org/signal-media/cyber-edge/offensive-cyber-operations-national-security-imperative (staženo 23. 11. 2023).

[93] Jason Lau, "State of Cybersecurity 2023: Navigating Current and Emerging Threats," ISACA, 2. 8. 2023, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/state-of-cybersecurity-2023-navigating-current-and-emerging-threats (staženo 24. 11. 2023).

Spojené státy nebo jejich spojenci vzdali kybernetické špionáže jako legitimního nástroje státní moci, ale mohlo by to stanovit ochranná pravidla pro to, co se považuje za cílené shromažďování zpravodajských informací, a co za ofensivní akce.[94]

Stanovení norem je přínosné také proto, že upozorňuje na používání ofensivních kybernetických schopností, které ovlivňují i jiné organizace než ty, na které se protivník snaží cílit. Zneužití zranitelnosti nultého dne (označení pro útok nebo hrozbu, která se snaží využít zranitelnosti používaného softwaru, která není ještě obecně známá a tím pádem proti ni zatím neexistuje obrana), často vede k rychlému zneužití dříve, než se ji podaří zastavit, což uvidíme později v textu na případu serveru Microsoft Exchange v březnu 2021. Mezinárodním normám chování v kyberprostoru byla v posledních letech věnována velká pozornost, ale slibný konsenzus z jednání OSN selhal poměrně rychle, jelikož není jasné, zda by země, jako je Rusko a Čína, tyto normy dodržovaly, pokud by za jejich nedodržení nebyly stanoveny tvrdé sankce, na čemž se země nebyly schopné domluvit. Spojené státy, Velká Británie, Evropská komise a NATO v červenci 2021 vyzvali Čínu k neofenzivnímu kybernetickému chování, avšak čínské ministerstvo zahraničí tato jakákoli nařknutí odmítlo a ukázalo prstem zpět na Spojené státy. Ačkoli se může zdát, že když se nepodařilo dosáhnout požadovaného výsledku, celá tato iniciativa byla zbytečná, avšak není tomu tak - představuje důležitý první krok k zaujetí pevnějšího postoje vůči takovým aktivitám. Spojené státy prokázaly, že chtějí spolupracovat se spojenci a partnery. Koordinované diplomatické úsilí upozorňující na tyto incidenty by mělo pokračovat, už jen proto, aby donutilo útočící země zodpovídat se ze svých činů.[95]

V květnu 2017 představoval útok ransomwaru WannaCry obrovskou výzvu v oblasti kybernetické bezpečnosti na celém světě a vyžádal si i reakci Spojených států. Přístup americké vlády kombinoval okamžité řešení krize se strategickou vizí dlouhodobé kybernetické odolnosti. Agentury včetně DHS, FBI a NSA se rychle zmobilizovaly, aby

[94] The White House, "FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," 12. 5. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ (staženo 24. 11. 2023).

[95] Pieter Arntz, "US, EU, UK, NATO blame China for 'reckless' Exchange attacks," Malwarebytes, 20. 6. 2021, https://www.malwarebytes.com/blog/news/2021/07/us-eu-uk-nato-blame-china-for-reckless-exchange-attacks (staženo 24. 11. 2023).

útok vyhodnotily a zvládly. Jejich koordinované úsilí se zaměřilo na pochopení mechanismů útoku WannaCry a poskytnutí okamžitých strategií pro zmírnění následků postiženým subjektům. Tato rychlá reakce měla zásadní význam pro omezení šíření ransomwaru a minimalizaci jeho dopadu na kritickou infrastrukturu a služby. US-CERT vydal varování a pokyny, sehrál klíčovou roli v informování veřejnosti i soukromého sektoru o této hrozbě. Tato komunikace měla zásadní význam pro zvyšování povědomí a doporučení pomohla organizacím i jednotlivcům přijmout rychlá opatření na ochranu před ransomwarem, například aplikovat bezpečnostní záplaty a zálohovat data. Krize si vyžádala jednotnou reakci různých vládních subjektů, která poukázala na důležitost spolupráce při řešení národních kybernetických bezpečnostních hrozeb.[96]

Vláda USA se po události WannaCry prioritně zaměřila na posílení své kybernetické bezpečnostní infrastruktury. To zahrnovalo modernizaci systémů, zavedení robustnějších kyberbezpečnostních opatření a zajištění průběžného monitorování a údržby. Pozornost byla zaměřena také na zabezpečení odvětví kritické infrastruktury, protože si uvědomuje jejich zranitelnost vůči takovým útokům a jejich význam pro národní bezpečnost. Cílem těchto snah bylo vytvořit jednotnější a komplexnější přístup k národní kybernetické bezpečnosti a překlenout mezery, které útok WannaCry využil.[97]

Vzhledem k tomu, že kybernetické hrozby se stále vyvíjejí, došlo k výraznému navýšení finančních prostředků na výzkum a vývoj v oblasti kybernetické bezpečnosti. Cílem této investice bylo udržet náskok USA v oblasti technologií a strategií kybernetické bezpečnosti a zajistit tak připravenost na budoucí kybernetické hrozby.[98]

---

[96] Cybersecurity & Infrastructure Security Agency, "Indicators Associated With WannaCry Ransomware, naposledy upraveno 6. 7. 2018, https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware (staženo 25. 11. 2023).
Department of Homeland Security, "DHS Statement on Ongoing Ransomware Attacks," 12. 5. 2017, https://www.dhs.gov/news/2017/05/12/dhs-statement-ongoing-ransomware-attacks (staženo 25. 11. 2023).

[97] Charles H. Romine, "Bolstering Government Cybersecurity: Lessons Learned from WannaCry," testimony before the Committee on Science, Space, and Technology, U.S. House of Representatives, 15. 6. 2017, https://www.nist.gov/speech-testimony/bolstering-government-cybersecurity-lessons-learned-wannacry (staženo 25. 11. 2023).
The White House, "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware," 13. 10. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ (staženo 25. 11. 2023).

[98] David Burg a Sean Joyce, "Cybersecurity after WannaCry: How to Resist Future Attacks," *Strategy+Business*, 16. 5. 2017, https://www.strategy-business.com/blog/Cybersecurity-After-WannaCry-How-to-Resist-Future-Attacks (staženo 25. 11. 2023).

Globální rozsah útoku WannaCry zdůraznil význam mezinárodní spolupráce v oblasti kybernetické bezpečnosti. Spojené státy zintenzivnily úsilí o spolupráci se spojenci a mezinárodními orgány, sdílení zpravodajských informací a strategií s cílem společně posílit obranu proti globálním kybernetickým hrozbám. Incident zdůraznil potřebu zvýšit povědomí o kybernetické bezpečnosti a vzdělávání veřejnosti i organizací.

V roce 2017 měl kybernetický útok NotPetya, jeden z nejničivějších v historii, těžké následky po celém světě, včetně významných dopadů ve Spojených státech. Reakce americké vlády na tento sofistikovaný malware, považovaný za státem sponzorovaný útok z Ruska, byla komplexní a zahrnovala okamžité krizové řízení a strategické dlouhodobé úpravy politiky kybernetické bezpečnosti. Na vyhodnocení útoku se podílely především Ministerstvo vnitřní bezpečnosti (DHS), Federální úřad pro vyšetřování (FBI) a Národní bezpečnostní agentura (NSA). DHS poskytovalo pokyny a podporu postiženým subjektům, zatímco FBI a NSA pracovaly na identifikaci pachatelů a pochopení technických aspektů malwaru. Vysoká úroveň koordinace a sdílení informací mezi americkými vládními agenturami usnadnila řešení útoku. To zahrnovalo kombinaci zdrojů a odborných znalostí různých zpravodajských služeb a subjektů zabývajících se kybernetickou bezpečností. Dále se vláda zaměřila na určení rozsahu škod, zejména na kritické infrastruktuře a klíčových odvětvích. Rychlé posouzení bylo klíčové pro formulaci reakce na bezprostřední krizi a pro předcházení dalším škodám. Při vydávání včasných a podrobných upozornění hrál klíčovou roli tým US-CERT. Tato sdělení poskytla veřejnému i soukromému sektoru zásadní informace o malwaru, jeho dopadu a strategiích zmírnění následků. Vládní komunikační strategie měla zásadní význam pro informování organizací a veřejnosti o závažnosti hrozby a o krocích potřebných k ochraně před takto sofistikovanými útoky. Byla posílena partnerství veřejného a soukromého sektoru s cílem vytvořit robustnější a odolnější infrastruktury kybernetické bezpečnosti, sdílet zpravodajské informace o hrozbách a spolupracovat na řešeních kybernetické bezpečnosti.[99]

Diego Laje and Nuray Taylor, "U.S. To Increase Cyber Capabilities, Research and Funding with NATO," *AFCEA International*, 29. 6. 2022, https://www.afcea.org/signal-media/us-increase-cyber-capabilities-research-and-funding-nato (staženo 25. 11. 2023).

[99] Jessica Davis, "DOJ Indicts Russian Hackers Behind 2017 NotPetya Malware Attack," *HealthITSecurity*, 20 8. 2020, https://www.healthitsecurity.com/news/doj-indicts-russian-hackers-behind-2017-notpetya-malware-attack/ (staženo 27. 11. 2023).

Po důkladném vyšetřování americká vláda ve spolupráci se svými spojenci připsala útok NotPetya ruské vládě. Toto připsání bylo významné pro zarámování útoku nejen jako kriminálního činu, ale jako geopolitické záležitosti. Reakce zahrnovala diplomatická opatření, jako je uvalení sankcí na Rusko a veřejné odsouzení útoku. Tato opatření sloužila jako odstrašující prostředek proti budoucím kybernetickým útokům sponzorovaným státem a zdůraznila postoj USA k mezinárodním kybernetickým normám. Globální charakter útoku NotPetya posílil potřebu mezinárodní spolupráce v oblasti kybernetické bezpečnosti. USA se zapojily do společného úsilí se spojenci a mezinárodními organizacemi s cílem zlepšit kolektivní schopnosti v oblasti kybernetické bezpečnosti. Spojené státy hrály klíčovou roli při vedení mezinárodních diskusí o kybernetických normách a společných reakcích na kybernetické hrozby a uvědomovaly si důležitost jednotného globálního přístupu ke kybernetické bezpečnosti. [100]

Reakce americké vlády na kybernetický útok SolarWinds v roce 2020, sofistikovaný a rozsáhlý útok připisovaný ruské zahraniční zpravodajské službě, zahrnovala několik federálních agentur a kladla důraz na koordinaci se soukromým sektorem. Tato reakce zdůraznila nutnost důrazných opatření federálního a soukromého sektoru k řešení kybernetických bezpečnostních hrozeb.[101]

V roce 2020 oznámila společnost FireEye, známá svou podporou při řešení kybernetických incidentů pro řadu společností a organizací, že se sama stala obětí kybernetického útoku. Hackerům se podařilo ukrást nástroje společnosti FireEye a zjevně se snažili naučit, jak je zneužít k průniku do jiných sítí. Společnosti FireEye se podařilo vystopovat chybu v aktualizaci jejich softwarového nástroje Orion, který využívají pro správu infrastruktury informačních technologií společnosti SolarWinds. Vláda spojených států povolala Jednotnou koordinační skupinu pro kybernetiku (UCG), aby koordinovala reakci na kompromitaci společnosti SolarWinds. Záhy se ukázalo, že obětí útoku se stalo více vládních agentur a společností ze soukromého sektoru. Analytici dospěli k závěru, že za kompromitaci jsou pravděpodobně zodpovědní ruští kybernetičtí aktéři a nastupující

[100] "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," U.S. Department of the Treasury, 15. 3. 2018, https://home.treasury.gov/news/press-releases/sm0312 (staženo 27. 11. 2023).
[101] "Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents," *U.S. Government Accountability Office*, GAO-22-104746, 13. 1. 2022, https://www.gao.gov/products/gao-22-104746 (staženo 27. 11. 2023).

Bidenova administrativa odhalila, že obětí se stalo devět vládních agentur a 100 společností. Mezi oběťmi bylo i ministerstvo financí, Národní úřad pro jadernou bezpečnost (NNSA, součást ministerstva energetiky) a ministerstvo vnitřní bezpečnosti.[102]

Odhalení společnosti FireEye bylo klíčové pro odhalení rozsahu narušení, což vedlo k širšímu povědomí o této hrozbě. Kromě toho sehrála zásadní roli společnost Microsoft, která oznámila, že útočník napadl některé z jejích cloudových platforem, což přispělo ke komplexnějšímu pochopení rozsahu útoku. Útok byl zaměřen na napadení aktualizací softwaru Orion společnosti SolarWinds, což umožnilo neoprávněný přístup do sítí a systémů zákazníků společnosti SolarWinds, včetně klíčových federálních vládních subjektů. Hlavním cílem útočníků byla zřejmě špionáž.[103]
V návaznosti na kompromitaci SolarWinds vydal Bílý dům dva exekutivní příkazy, včetně příkazu z 15. dubna 2021, jehož cílem bylo řešit "škodlivé zahraniční aktivity Ruska". Tento příkaz se týká obecně škodlivých kybernetických aktivit, nikoli konkrétně špionáže. Kompromitace společnosti SolarWinds nebyla prvním případem, kdy se vláda Spojených států stala obětí kybernetické kompromitace, a pravděpodobně nebude ani posledním.[104]

CISA reagovala okamžitě a proaktivně, když vydala nouzovou směrnici, v níž nastínila nezbytná opatření pro federální úřady. Tato směrnice měla zásadní význam pro vedení federálních subjektů při prevenci dalšího zneužívání. V dalším kroku došlo k vytvoření jednotné koordinační skupiny pro kybernetiku. Národní bezpečnostní rada aktivovala tuto skupinu složenou z klíčových zpravodajských agentur a agentur pro kybernetickou bezpečnost, aby vedla reakci na federální úrovni. Jejich společné úsilí bylo klíčové pro účinné zvládnutí incidentu. CISA vydala několik doporučení, včetně aktualizace

[102] "The SolarWinds Cyber-Attack: What You Need to Know," *Center for Internet Security (CIS)*, 15. 3. 2021, https://www.cisecurity.org/solarwinds (staženo 27. 11. 2023).
[103] Sam Ingalls, "FireEye, SolarWinds Breaches: Implications and Protections," *eSecurity Planet*, 18. 12. 2020, https://www.esecurityplanet.com/threats/fireeye-solarwinds-breaches-implications-protections/ (staženo 27. 11. 2023).
[104] The White House, "FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," 12. 5. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ (staženo 28. 11. 2023).
"FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," *The White House*, 14. 4. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (staženo 28. 11. 2023).

zranitelných systémů pomocí záplat poskytovaných společností SolarWinds a zavedení osvědčených postupů v oblasti kybernetické bezpečnosti, jako je například spouštění softwaru s neprivilegovaným přístupem.[105]

Mezi nástroje poskytnuté společností FireEye a Mandiant patřila bílá kniha se strategiemi zabezpečení pro Microsoft 365 a skript pro audit cloudu Azure. Tyto zdroje pomohly organizacím identifikovat a zmírnit potenciální ohrožení.[106]

Kongres se rovněž aktivně zapojil do snahy o pochopení hackerského útoku na společnost SolarWinds prostřednictvím několika slyšení, na nichž zdůraznil význam bezpečnosti dodavatelského řetězce informačních technologií a diskutoval o možných zlepšeních federálních postupů v oblasti kybernetické bezpečnosti.[107]

Reakce americké vlády na hackerské útoky na server Microsoft Exchange v roce 2021, které byly připsány čínským vládním pobočkám, zahrnovala koordinaci mezi různými federálními agenturami a mezinárodními spojenci. Cílem této reakce bylo řešit sofistikovanou kyberšpionážní operaci a zvýšit celkovou odolnost kybernetické bezpečnosti. Spojené státy vytvořily koalici se spojenci, včetně Evropské unie, Spojeného království a NATO, aby společně odhalily a kritizovaly kybernetické aktivity Čínské lidové republiky. Tato spolupráce podtrhuje globální přístup ke sdílení informací o kybernetických hrozbách, síťové obraně a společnému postupu proti bezpečnostním a ekonomickým hrozbám. Toto veřejné připsání bylo významné pro demonstraci jednotné fronty proti státem podporovaným kybernetickým aktivitám a zdůraznilo potřebu

[105] "CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products," *Cybersecurity and Infrastructure Security Agency*, 13. 12. 2020, https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network (staženo 30. 11. 2023).
"Supply Chain Compromise," *Cybersecurity and Infrastructure Security Agency*, 7. 1. 2021, https://www.cisa.gov/news-events/alerts/2021/01/07/supply-chain-compromise (staženo 30. 11. 2023).
[106] Mike Burns, Matthew McWhirt, Douglas Bienstock, Nick Bennett, a Juraj Sucik, "Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452," *Mandiant Blog*, 19. 1. 2021, https://www.mandiant.com/resources/blog/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452 (staženo 30. 11. 2023).
[107]"SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)," *U.S. Government Accountability Office Blog*, 22. 4. 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (staženo 30. 11. 2023).

odpovědného chování státu v kyberprostoru.[108]

Agentury včetně CISA, FBI, ODNI a NSA vytvořily skupiny pro koordinovanou reakci. Incidenty zdůraznily účinnost spolupráce veřejného a soukromého sektoru a význam centralizované komunikace v oblasti kybernetické bezpečnosti. Upozornily však také na problémy, jako je pomalé sdílení informací a omezení při shromažďování důkazů v důsledku rozdílných postupů uchovávání údajů v jednotlivých agenturách. Integrace partnerů ze soukromého sektoru v rámci skupiny Microsoft Exchange znamenala vývoj partnerství veřejného a soukromého sektoru v oblasti kybernetické bezpečnosti a potvrdila klíčovou roli soukromých subjektů v kybernetické obraně.[109]

Tyto agentury vydaly nouzové směrnice pro federální úřady, v nichž podrobně popisují potřebné kroky k posílení zranitelných míst. Poskytly komplexní poradenství týkající se technik a schopností aktérů hrozeb a usnadnily agenturám zabezpečení jejich sítí.[110]

V reakci na tento útok vláda USA upřednostnila financování modernizace kybernetické bezpečnosti ve všech federálních subjektech. To zahrnovalo vylepšení, jako je lepší zabezpečení koncových bodů a modernizace bezpečnostních operačních center, což zdůrazňuje závazek posílit národní infrastrukturu kybernetické bezpečnosti proti sofistikovaným hrozbám.[111]

Tento incident nejenže formoval strategie kybernetické bezpečnosti USA, ale měl také trvalé důsledky pro globální přístup k řízení a zmírňování kybernetických hrozeb.

---

[108] "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," *The White House*, 19. 6. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/ (staženo 30. 11. 2023).

[109] "Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents," *U.S. Government Accountability Office*, GAO-22-104746, 13. 1. 2022, https://www.gao.gov/products/gao-22-104746 (staženo 1. 12. 2023).

[110] Ibidem.

[111] "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," *The White House*, 19. 6. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/ (staženo 1. 12. 2023).

3.3 Kybernetické incidenty ve Spojeném království a jeho reakce

Do reakce Spojeného království na kybernetické hrozby je zapojena celá řada institucí. To zahrnuje různé vládní resorty, agentury a organizace, které mezi sebou spolupracují. Mezi tyto instituce patří Vládní komunikační ústředna (GCHQ), Národní centrum kybernetické bezpečnosti (NCSC), zpravodajské agentury, Národní agentura pro boj proti trestné činnosti (NCA) a další vládní úřady související se sociální politikou, digitalizací, kulturou, médii, obchodem a obranou.

Národní program kybernetické bezpečnosti (NCSP) hraje klíčovou roli při zvyšování národní kybernetické bezpečnosti a boji proti kybernetické kriminalitě. Zaměřuje se na zlepšování celkových schopností v oblasti kybernetické bezpečnosti, podporu úsilí v oblasti prosazování práva a podporu informovanosti veřejnosti. NCSP investuje do výzkumu a vývoje, podporuje inovace v odvětví kybernetické bezpečnosti a poskytuje podnikům finanční prostředky a poradenství pro zlepšení jejich kybernetických bezpečnostních opatření. GCHQ je zodpovědná za ochranu vládních systémů a podporu orgánů činných v trestním řízení při vyšetřování kybernetické kriminality. NCSC zase slouží jako hlavní vládní zdroj odborných znalostí v oblasti kybernetiky a úzce spolupracuje s průmyslem a akademickou obcí.[112]

Vláda Spojeného království problematiku kybernetických hrozeb řeší posilováním spolupráce, zvyšováním informovanosti podniků a podporou ochrany podniků a firem. V úsilí Spojeného království o kybernetickou bezpečnost je rovněž kladen důraz na právní rámec a odpovědnost, což zajišťuje, že instituce jako GCHQ a NCSC fungují v rámci britského práva a přenesených pravomocí. Vláda Spojeného království věnuje větší pozornost kybernetické bezpečnosti od poloviny roku 2000, což vyvrcholilo vytvořením Národního programu kybernetické bezpečnosti (NCSP) v roce 2010. Cílem tohoto programu je bránit zemi před kybernetickými útoky, odrazovat potenciální útočníky a rozvíjet britský průmysl kybernetické bezpečnosti. Program NCSP je každoročně

[112] "National Cyber Security Centre, '2020 Annual Review," NCSC, 15. 3. 2021, https://www.ncsc.gov.uk/annual-review/2020/index.html (staženo 1. 12. 2023).

přezkoumáván a na podporu jeho cílů je vyčleněn značný rozpočet.[113]

Jedním z hlavních prvků NCSP je zlepšení národní kybernetické bezpečnosti. To zahrnuje posílení ochrany kritické infrastruktury, jako jsou energetické, dopravní a komunikační systémy, které jsou zranitelné vůči kybernetickým hrozbám. Posílení kybernetické obrany v těchto odvětvích má zásadní význam pro zabezpečení základních služeb v zemi. Další oblastí, na kterou se NCSP zaměřuje, je boj proti kybernetické kriminalitě. Vzhledem k tomu, že kybernetická kriminalita ve Spojeném království převyšuje všechny ostatní formy trestné činnosti, je řešení tohoto problému zásadní. Úsilí v boji proti kybernetické kriminalitě zahrnuje spolupráci mezi donucovacími orgány, zpravodajskými službami a dalšími vládními úřady při vyšetřování a stíhání kybernetických zločinců. Nedílnou součástí účinného boje proti kybernetické kriminalitě je také zvyšování povědomí, vzdělávání a rozvoj dovedností v oblasti kybernetické bezpečnosti.[114]

Kromě toho se NCSP zaměřuje na zlepšení vzdělávání a dovedností souvisejících s kybernetickou bezpečností. To zahrnuje poskytování školení a vzdělávacích programů s cílem vytvořit kvalifikovanou pracovní sílu schopnou účinně reagovat na kybernetické hrozby. Celkově slouží NCSP jako rámec pro koordinaci mnoha organizací zapojených do řešení kybernetických hrozeb a zajištění bezpečnosti kybernetického prostoru Spojeného království. Zaměřením na zlepšení národní kybernetické bezpečnosti, obranu kritické infrastruktury, boj proti kybernetické kriminalitě a zlepšení vzdělávání a dovedností se vláda Spojeného království snaží vytvořit robustní a odolný systém kybernetické bezpečnosti.[115]

Národní program kybernetické bezpečnosti ve Spojeném království má čtyři hlavní cíle - zlepšit národní kybernetickou bezpečnost, posílit schopnosti prosazování práva, rozvíjet průmysl kybernetické bezpečnosti a utvářet mezinárodní prostředí kybernetické

[113]"Cabinet Office and Department for Business, Innovation & Skills, '2010 to 2015 Government Policy: Cyber Security", UK Government, 8. 5. 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security (staženo 1. 12. 2023).
[114] Kristan Stoddart, "UK cyber security and critical national infrastructure protection", International Affairs, Volume 92, Issue 5, 31. 8. 2016, strany 1079–1105, https://academic.oup.com/ia/article-abstract/92/5/1079/2688134?redirectedFrom=fulltext (staženo 2. 12. 2023).
[115] "Government Digital Service", Cyber skills for a vibrant and secure UK.' GOV.UK. 12. 12. 2014. https://www.gov.uk/government/news/cyber-skills-for-a-vibrant-and-secure-uk (staženo 2. 12. 2023).

bezpečnosti.[116]

Vláda Spojeného království zřídila v souvislosti s řešením kybernetické kriminality a jejího dopadu na podniky několik organizací a iniciativ. Vládní komunikační ústředí (GCHQ) je zodpovědné za ochranu vládních systémů a podporu orgánů činných v trestním řízení při řešení kybernetických hrozeb. Národní centrum kybernetické bezpečnosti (NCSC) slouží jako hlavní zdroj odborných znalostí vlády v oblasti kybernetické problematiky a spolupracuje s průmyslem a akademickou obcí. Do boje proti kybernetické kriminalitě je zapojena také Národní agentura pro boj proti kriminalitě (NCA). Vláda klade důraz na ochranu podniků a firem a považuje kybernetickou bezpečnost za klíčový aspekt celkové bezpečnosti.[117]

Vláda Spojeného království si celkově uvědomuje důležitost koordinované reakce na kybernetické hrozby a klade důraz na ochranu podniků a průmyslu. V květnu 2017 čelila Velká Británie závažnému problému v oblasti kybernetické bezpečnosti, když útok ransomwaru WannaCry vážně zasáhl Národní zdravotní službu (NHS). Reakce vlády na tuto krizi byla mnohostranná a ukázala odhodlání k okamžitým opatřením i k dlouhodobé strategické reformě v oblasti kybernetické bezpečnosti.[118]

Počáteční reakce se vyznačovala rychlým omezením šíření viru. NHS s pomocí Národního centra kybernetické bezpečnosti (NCSC) okamžitě izoloval infikované systémy, aby zabránil dalšímu šíření ransomwaru. Tato rychlá akce byla klíčová pro omezení škod. NCSC, které je součástí britského Vládního komunikačního ústředí (GCHQ), sehrálo klíčovou roli a poskytlo technické odborné znalosti a podporu. Koordinovalo svou činnost s mezinárodními subjekty zabývajícími se kybernetickou bezpečností a sdílelo informace a strategie boje proti útoku. Současně byl kladen velký důraz na komunikaci s veřejností.

---

[116] "Progress of the 2016-2021 National Cyber Security Programme", National Audit Office (NAO). 15. 3. 2019, https://www.nao.org.uk/press-releases/progress-of-the-2016-2021-national-cyber-security-programme/ (staženo 2. 12. 2023).

[117] "NCSC Annual Review 2020", National Cyber Security Centre, https://www.ncsc.gov.uk/annual-review/2020/index.html (staženo 2. 12. 2023).
"Cyber Crime", National Crime Agency, https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime (staženo 2. 12. 2023).

[118] "Investigation: WannaCry cyber attack and the NHS", National Audit Office (NAO), 27. 10. 2017, https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/.https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/ (staženo 2. 12. 2023).

Vláda a představitelé NHS neprodleně informovali veřejnost o povaze a rozsahu útoku, o snaze zmírnit jeho dopady a o radách pro pacienty během přerušení provozu. Tato komunikace měla zásadní význam pro udržení důvěry veřejnosti a minimalizaci paniky.[119]

Vláda Spojeného království provedla po výskytu viru WannaCry komplexní revizi své kybernetické bezpečnosti, přičemž se zaměřila zejména na NHS. To vedlo k významným změnám politiky a investicím. Vláda vyčlenila značné finanční prostředky na posílení infrastruktury kybernetické bezpečnosti NHS. Tyto investice byly zaměřeny na modernizaci zastaralých systémů, které byly během útoku identifikovány jako klíčová zranitelná místa. Důraz byl kladen na zavedení pokročilých nástrojů kybernetické bezpečnosti a zajištění pravidelných aktualizací. Incident urychlil důkladné přezkoumání stávajících zásad kybernetické bezpečnosti. Byly vypracovány nové, robustnější strategie, které se zaměřují nejen na obranu proti podobným útokům, ale také na přípravu na nové kybernetické hrozby. Tato revize politiky představovala posun od reaktivního k proaktivnímu řízení kybernetické bezpečnosti. V tomto případě bylo také zřetelné, že na úspěchu kybernetických útoků se často podílí lidský faktor, a proto také vláda zahájila rozsáhlé školicí programy pro zaměstnance NHS. Cílem těchto programů bylo zvýšit povědomí o rizicích kybernetické bezpečnosti a osvědčených postupech, a posílit tak první linii obrany. Vláda také vedla nezávislá vyšetřování, aby analyzovala útok a reakci na něj. Tato vyšetřování přinesla zásadní poznatky a doporučení pro posílení kybernetických bezpečnostních opatření. Zprávy zdůraznily potřebu neustálého vyhodnocování a přizpůsobování strategií kybernetické bezpečnosti s ohledem na vyvíjející se hrozby.[120]

Útok WannaCry zdůraznil potřebu spolupráce v oblasti kybernetické bezpečnosti. Vláda Spojeného království posílila spolupráci s mezinárodními partnery s cílem sdílet znalosti, strategie a zpravodajské informace. Cílem tohoto globálního přístupu bylo posílit kolektivní obranu proti kybernetickým hrozbám. Reakce britské vlády na útok ransomwaru WannaCry byla kombinací okamžitých taktických opatření a strategických dlouhodobých

[119] "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS," *npj Digital Medicine* 2, no. 98 (2019), https://doi.org/10.1038/s41746-019-0161-6 (staženo 2. 12. 2023).
[120] Department of Health and Social Care, "Government Sets Out Strategy to Protect NHS from Cyber Attacks,"naposledy upraveno 12. 6. 2021, https://www.gov.uk/government/news/government-sets-out-strategy-to-protect-nhs-from-cyber-attacks (staženo 2. 12. 2023).
Saira Ghafur, Guy Martin, J. James Kinross, Chris Hankin, a Ara Darzi,"WannaCry—a Year On," *BMJ* 361 (2018): k2381, https://doi.org/10.1136/bmj.k2381 (staženo 2. 12. 2023).

změn.

V roce 2017 čelila vláda Spojeného království další výzvě v oblasti kybernetické bezpečnosti v souvislosti s útokem NotPetya. Tento sofistikovaný malware, který ovlivnil organizace po celém světě, vyžadoval rychlou a strategickou reakci Spojeného království s cílem zmírnit jeho dopady a posílit budoucí odolnost. Národní centrum kybernetické bezpečnosti (NCSC) bylo spolu s dalšími vládními agenturami rychle mobilizováno. Úloha NCSC byla klíčová při organizování koordinované reakce, vyhodnocování dopadu malwaru a určování prioritních opatření pro kritická odvětví.[121]

Podobně jako v reakci na vir WannaCry byly podniknuty okamžité kroky k omezení šíření malwaru a zmírnění jeho dopadu, zejména v odvětvích, jako je zdravotnictví a obchod. NCSC poskytl těmto sektorům technické odborné znalosti a podporu při zvládání útoku a zotavení z něj. NCSC vydala včasná upozornění pro veřejný i soukromý sektor s podrobnými informacemi o povaze útoku, ochranných opatřeních a krocích k obnově. Tyto informace byly pro organizace zásadní, aby mohly účinně reagovat a minimalizovat škody. Útok zdůraznil význam jednotné národní reakce, do níž by se zapojily různé vládní orgány. Toto společné úsilí umožnilo komplexnější a účinnější zvládnutí kybernetického incidentu. Po výskytu viru NotPetya bylo vyvinuto společné úsilí o přehodnocení a revizi národních strategií kybernetické bezpečnosti. Tento přezkum odhalil mezery ve stávajících rámcích a byl podkladem pro vypracování robustnějších politik kybernetické bezpečnosti. Incident ovlivnil diskuse o legislativě a zdůraznil potřebu přísnějších zákonů a předpisů na ochranu před tak sofistikovanými kybernetickými hrozbami a zajištění odolné digitální infrastruktury.[122]

Spojené království se připojilo ke svým spojencům a veřejně připsalo útok NotPetya ruské vládě. Tento krok byl významný z hlediska mezinárodní kybernetické diplomacie a postavení proti státem sponzorovaným kybernetickým aktivitám. Spojené království se po

[121] National Cyber Security Centre, "Russian Military Almost Certainly Responsible for Destructive 2017 Cyber Attack", naposledy upraveno 17. 2. 2018, https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack (staženo 2. 12. 2023).
[122] Foreign & Commonwealth Office a Lord (Tariq) Ahmad of Wimbledon, "Foreign Office Minister Condemns Russia for NotPetya Attacks," naposledy upraveno 15. 2. 2018, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (staženo 2. 12. 2023).

atribuci zapojilo do diplomatických opatření, čímž posílilo svůj závazek dodržovat mezinárodní kybernetické normy a odstrašující strategie proti kybernetické agresi ze strany národních států.[123]

V roce 2020 si kybernetický útok společnosti SolarWinds, sofistikovaný průnik do dodavatelského řetězce, který zasáhl řadu globálních subjektů včetně těch ve Spojeném království, vyžádal od britské vlády opět velmi komplexní reakci. Přijatá strategie byla kombinací okamžité akce, koordinované reakce, přehodnocení politiky a dlouhodobého strategického plánování. NCSC se ujalo vedení při zjišťování rozsahu infiltrace ve Spojeném království. To zahrnovalo identifikaci systémů a dat, které mohly být ohroženy, se zvláštním zaměřením na vládní sítě a kritickou infrastrukturu. Posouzení se rovněž zaměřilo na pochopení potenciálních rizik pro národní bezpečnost a citlivé údaje, což je zásadní pro stanovení následných reakčních opatření. Při reakci byl použit integrovaný přístup zahrnující různé britské zpravodajské služby a agentury pro kybernetickou bezpečnost. Tato koordinace zajistila jednotnou a komplexní národní reakci na komplexní kybernetickou hrozbu.[124]

Při vyšetřování tohoto útoku Spojené království úzce spolupracovalo s mezinárodními spojenci, zejména se Spojenými státy, které byly rovněž významně zasaženy. Toto partnerství bylo klíčové při sdružování zdrojů, zpravodajských informací a odborných znalostí, což umožnilo širší pochopení mechanismů a původu útoku.[125]

NCSC aktivně oslovila potenciálně zasažené organizace a nabídla jim podrobné pokyny k identifikaci a zmírnění případných narušení. Tato podpora se rozšířila nejen na vládní subjekty, ale i na organizace soukromého sektoru. Pravidelně také byla vydávána doporučení, aby byly všechny zúčastněné strany informovány o osvědčených postupech

[123] Foreign & Commonwealth Office a Lord (Tariq) Ahmad of Wimbledon, "Foreign Office Minister Condemns Russia for NotPetya Attacks," naposledy upraveno 15. 2. 2018, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (staženo 2. 12. 2023).
[124] National Cyber Security Centre, "NCSC Statement on SolarWinds Compromise,", National Cyber Security Centre, "UK and US Call Out Russia for SolarWinds Compromise," https://www.ncsc.gov.uk/news/ncsc-statement-on-solarwinds-compromise (staženo 5. 12. 2023).
[125] Ibidem.

pro zabezpečení svých systémů proti zranitelnostem zneužitým při útoku.[126]

Vláda Spojeného království prostřednictvím Úřadu pro zahraničí oficiálně odhalila zapojení civilní zahraniční zpravodajské služby Ruské federace (SVR) do kompromitace společnosti SolarWinds. SVR je známá svými vysokými technologickými schopnostmi a zaměřuje se na různé subjekty pro zpravodajské účely. Toto odhalení bylo zásadním krokem k uznání hrozby a vyvození odpovědnosti. Ačkoli celkový dopad na Spojené království i Spojené státy byl spíše středního rozsahu, vlády postupovaly velice ostražitě, zejména proto, že operace SVR zahrnovaly přístup do vládních sítí v Evropě a členských zemích NATO za účelem shromažďování zpravodajských informací. Tato společná reakce byla součástí širšího souboru opatření, včetně sankcí a dalších opatření namířených proti Rusku, přijatých s cílem uvalit na něj sankce za jeho škodlivé aktivity proti suverenitě a zájmům ostatních států. Součástí reakce bylo také vyhoštění personálu a cílené sankce proti subjektům napojeným na ruské zpravodajské služby.[127]

Ačkoli Spojené království odsoudilo jednání Ruska a připojilo se k USA ve formální odpovědnosti, zdá se, že se rozhodlo spíše pro politiku "pojmenování a zahanbení" než pro odvetná opatření. To naznačuje opatrnější přístup, který se zaměřuje spíše na odhalování a diplomatické kanály než na přímou finanční nebo diplomatickou odvetu.[128]

Reakce britské vlády na útok SolarWinds byla důkazem nutnosti dynamického, vícevrstvého přístupu k řešení komplexních kybernetických hrozeb. Efektivním zvládnutím bezprostřední krize, zapojením do národní a mezinárodní spolupráce, revizí politik a zaměřením se na dlouhodobý strategický vývoj.

Dalším důležitým momentem byla reakce britské vlády na hackerský útok na server

[126] Mark Say, "NCSC Publishes Guidance on Responses to Cyber Attacks," UKAuthority, naposledy upraveno 2. 11. 2020, https://www.ukauthority.com/articles/ncsc-publishes-guidance-on-responses-to-cyber-attacks/ (staženo 5. 12. 2023).
[127] Neil Ashdown, "UK and US Confirm Russian Responsibility for SolarWinds Attack," Jane's Defence News, 6. 5. 2021, https://www.janes.com/defence-news/news-detail/uk-and-us-confirm-russian-responsibility-for-solarwinds-attack (staženo 5. 12. 2023).
[128] Jamie MacColl, "The UK's Approach to Russian Cyber Operations Shows No Signs of Changing," Royal United Services Institute, 21. 5. 2021, https://www.rusi.org/explore-our-research/publications/commentary/uks-approach-russian-cyber-operations-shows-no-signs-changing (staženo 7. 12. 2023).

Microsoft Exchange v roce 2021. Spojené království spolu s mezinárodními partnery otevřeně obvinilo z organizování hackerského útoku čínským státem podporované subjekty, konkrétně skupiny Hafnium, APT40 a APT31. Tato veřejná atribuce byla zásadním krokem v reakci Spojeného království, protože nejen identifikovala pachatele, ale také vytvořila precedens pro transparentnost při řešení státem sponzorovaných kybernetických hrozeb. Otevřeným uvedením odpovědných stran se Spojené království postavilo do pozice proaktivního a transparentního aktéra v globálním prostředí kybernetické bezpečnosti.[129]

Koordinovaný postoj Spojeného království se spojenci, jako jsou USA, zdůraznil význam mezinárodní spolupráce při řešení kybernetických bezpečnostních hrozeb. Tato globální spolupráce odráží pochopení, že kybernetické hrozby nejsou omezeny hranicemi států, a proto vyžadují jednotnou mezinárodní reakci. Taková spolupráce může vést k účinnějším strategiím odstrašení a obrany proti podobným útokům v budoucnu a podpořit pocit sdílené odpovědnosti a kolektivní akce v kybernetické oblasti.[130]

Zapojení NCSC do poskytování poradenství více než 70 organizacím postiženým hackerským útokem podtrhuje závazek Spojeného království nejen řešit bezprostřední hrozby, ale také budovat dlouhodobou odolnost kybernetické bezpečnosti. Tento přístup přesahuje rámec pouhého krizového řízení - zahrnuje vzdělávání a vybavování podniků a institucí znalostmi a nástroji na obranu proti budoucím kybernetickým hrozbám. Opět, úloha NCSC je klíčová při vytváření bezpečnějšího digitálního prostředí ve Spojeném království.[131]

Zásadním aspektem reakce Spojeného království byla výzva, aby Čína dodržovala mezinárodní dohody a kybernetické normy. Zdůrazněním dohod, jako je závazek skupiny G20 z roku 2015 proti krádežím duševního vlastnictví v kyberprostoru, Spojené království

[129] Government of the United Kingdom, "UK and Allies Hold Chinese State Responsible for a Pervasive Pattern of Hacking," naposledy upraveno 19. 6. 2021, https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking (staženo 7. 12. 2023).
[130] OODA Loop, "UK Blames China for Microsoft Exchange Server Hack," OODA Loop, 19. 6. 2021, https://www.oodaloop.com/briefs/2021/07/19/uk-blames-china-for-microsoft-exchange-server-hack/ (staženo 7. 12. 2023).
[131] National Cyber Security Centre, "Advice Following Microsoft Vulnerabilities Exploitation," https://www.ncsc.gov.uk/news/advice-following-microsoft-vulnerabilities-exploitation (staženo 7. 12. 2023).

zdůraznilo význam dodržování zavedených mezinárodních norem. Tento diplomatický tlak nespočíval pouze v řešení bezprostředního problému, ale také v posílení globálního rámce, který upravuje chování států v kyberprostoru. Takové úsilí má zásadní význam pro utváření mezinárodního řádu založeného na pravidlech v digitální oblasti.[132]

Celkově byla reakce Spojeného království na narušení serveru Microsoft Exchange v roce 2021 velmi komplexní a zahrnovala prvky transparentnosti, mezinárodní spolupráce, institucionální odolnosti a diplomatické angažovanosti. Tento mnohostranný přístup svědčí o složitosti řešení moderních kybernetických hrozeb a zdůrazňuje potřebu koordinovaných reakcí, které zahrnují jak technické, tak diplomatické strategie.

4. Budoucí výzvy v kybernetické bezpečnosti

4.1 Aktuální trendy v oblasti kybernetické bezpečnosti

Nárůst kybernetické kriminality, úniků dat a hackerských útoků má dopad na jednotlivce i vlády po celém světě. Zprávy uvádějí nárůst 125% globálních kybernetických útoků od roku 2021, přičemž tento trend přetrval i v roce 2022 a zdůraznil naléhavou poptávku po posílení kybernetické bezpečnostní ochrany. Bezpečnostním odborníkům trvá v průměru přibližně 277 dní, než identifikují a neutralizují kybernetický útok, což poukazuje na složitou povahu efektivního řízení a zmírňování těchto digitálních hrozeb.[133]

Jedním z hlavních problémů, kterým budou tvůrci kybernetických politik v budoucnosti čelit bude zvyšující se složitost kybernetických hrozeb. Kybernetičtí útočníci neustále vyvíjejí své metody a používají sofistikované techniky, jako je umělá inteligence a strojové učení, aby obešli bezpečnostní opatření. Umělou inteligenci lze například využít k automatizaci útoků nebo vytváření přesvědčivějších phishingových e-mailů. Zavádění umělé inteligence na trhu kybernetické bezpečnosti roste složenou roční mírou růstu (CAGR) o 23,6 %. Očekává se, že do roku 2027 dosáhne tržní hodnoty 46,3 miliardy

[132] Government of the United Kingdom, "UK and Allies Hold Chinese State Responsible for a Pervasive Pattern of Hacking," naposledy upraveno 19. 6. 2021, https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking (staženo 9. 12. 2023).
[133] "A Year in Review: Cybersecurity Trends and Challenges in 2023," C8 Secure, 17. 11. 2023, https://www.c8secure.com/2023/11/17/a-year-in-review/ (staženo 9. 12. 2023).

dolarů. Menší podniky, organizace a zejména zdravotnická zařízení, které si nemohou dovolit tak vysoké investice do nejmodernějších technologií kybernetické bezpečnosti, jako je právě umělá inteligence, jsou obzvláště zranitelné. Aby mohly vlády těmto pokročilým hrozbám čelit, musí investovat do minimálně stejně pokročilých a často dražších řešení kybernetické bezpečnosti, jako jsou systémy detekce hrozeb založené na umělé inteligenci.[134]

S rozvojem internetu věcí (Internet of Things) prudce roste počet zařízení připojených k sítím, od chytrých domácích zařízení až po průmyslové senzory. Každé z těchto zařízení představuje potenciální vstupní bod pro útočníky. Zabezpečení tak rozmanité škály zařízení vyžaduje rovněž širokou škálu bezpečnostních nástrojů a strategií, jejichž implementace a údržba je samozřejmě nákladná. Zařízení internetu věcí mají často různé a nekonzistentní bezpečnostní protokoly - mnohá z nich nejsou vyvíjena s ohledem na bezpečnost jako na prioritu, což je činí mimořádně zranitelnými vůči útokům. Kromě toho je v oblasti bezpečnosti internetu věcí stále důležitější koncept nulové důvěryhodnosti. V systému nulové důvěryhodnosti musí být všechna zařízení a uživatelé před udělením přístupu ke zdrojům ověřeni a autentizováni. Tento přístup eliminuje implicitní důvěru a průběžně ověřuje každou fázi digitální interakce. Je třeba vést v patrnosti, že tato zařízení shromažďují obrovské množství osobních a citlivých údajů. Pokud je ohroženo zabezpečení, hrozí riziko úniku dat, což vede k porušení ochrany soukromí. Některá zařízení internetu věcí mohou být provozována na zastaralém softwaru, který nedostává pravidelné aktualizace, což je činí zranitelnými vůči novějším kybernetickým hrozbám. Zařízení internetu věcí jsou často vzájemně propojena, což znamená, že narušení jednoho zařízení může potenciálně ohrozit celou síť nebo systém.[135]

Nedostatek kvalifikovaných odborníků v oblasti kybernetické bezpečnosti rovněž značně stěžuje adekvátní vyvíjení a dodržování bezpečnostní kybernetické politiky. Kvalifikovaných odborníků na kybernetickou bezpečnost je celosvětově nedostatek. Tento nedostatek znamená, že náklady na nábor kvalifikovaných pracovníků v oblasti

[134] "A Year in Review: Cybersecurity Trends and Challenges in 2023," C8 Secure, 17. 11. 2023, https://www.c8secure.com/2023/11/17/a-year-in-review/ (staženo 9. 12. 2023).
[135] Viral Gandhi, "2023 ThreatLabz Report Indicates 400% Growth in IoT Malware Attacks," Zscaler Blog, 24. 10. 2023, https://www.zscaler.com/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks (staženo 9. 12. 2023).

kybernetické bezpečnosti jsou velmi vysoké, protože poptávka převyšuje nabídku. Podle studie ISC2 2023 Workforce Study 92 % společností hlásí nedostatek zaměstnanců ve svých organizacích, přičemž mezi tři nejčastěji chybějící dovednosti patří zabezpečení cloud computingu, umělá inteligence/strojové učení a implementace nulové důvěryhodnosti. Ekonomická nejistota vedla také ke snižování výdajů, a to i na školicí programy v oblasti kybernetické bezpečnosti, které mají zásadní význam pro rozvoj potřebných dovedností a růst pracovních sil. Tyto škrty měly negativní dopad na produktivitu, morálku týmů a zvýšily pracovní zátěž stávajících zaměstnanců, což problém ještě zhoršilo. Kybernetická bezpečnost vyžaduje neustálou ostražitost a systémy je třeba pravidelně aktualizovat, aby se chránily před novými hrozbami. Toto nepřetržité monitorování a potřeba rychlé reakce na incidenty vyžadují investice do technologií i personálu, což vede k vysokým provozním nákladům. Trend homeoffice také přinesl nové výzvy v oblasti kybernetické bezpečnosti. Ochrana dat a systémů v různých pracovních prostředích (například doma u zaměstnanců) vyžaduje flexibilní a často složitější bezpečnostní řešení.[136]

Vydírání prostřednictvím útoků ransomwaru zůstává trvalou a stále se vyvíjející hrozbou. Útočníci často požadují platby v kryptoměnách, což znesnadňuje následnou snahu o vypátrání peněz orgány činnými v trestním řízení. Tyto útoky nejen narušují chod podniků, ale vedou také ke značným finančním ztrátám a potenciálnímu poškození pověsti organizace. Společnosti musí investovat do preventivních opatření, jako jsou robustní zálohovací systémy a školení zaměstnanců, aby snížily riziko takových útoků.[137]

Společnost Chainalysis oznámila, že v první polovině roku 2023 výrazně vzrostl počet trestných činů souvisejících s ransomwarem v kryptoměnách, při nichž hakeři získali 450 milionů dolarů. V celosvětovém měřítku se 64 % organizací, které se staly terčem

[136] "ISC2, 'ISC2 Reveals Workforce Growth But Record-Breaking Gap: 4 Million Cybersecurity Professionals", ISC2.org, 23. 10. 2023, https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals (staženo 9. 12. 2023).
[137] "The Use of Bitcoin and Cryptocurrencies in Ransomware Attacks: Why Employers Should Care", Fisher Phillips, https://www.fisherphillips.com/en/news-insights/bitcoin-and-cryptocurrencies-ransomware-attacks.html (staženo 9. 12. 2023).
"Ransomware: The Data Exfiltration and Double Extortion Trends", CISecurity.org, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (staženo 10. 12. 2023).

ransomwaru, rozhodlo výkupné zaplatit. Pokud bude tento trend pokračovat, mohli by útočníci v roce 2023 získat téměř 900 milionů dolarů, čímž by překonali čísla z roku 2022. Lindy Cameron, vedoucí britského NCSC (National Cyber Security Centre), a John Edwards, komisař pro informace, však od placení výkupného odrazují, protože nezaručuje pozitivní výsledek. Oběti nemusí získat zpět přístup ke svým datům nebo počítačovým systémům a hrozba přetrvávajících hrozeb na jejích serverech zůstává. Placení výkupného může zvýšit zranitelnost společností vůči budoucím útokům.[138]

Phishing je pro hackery stále nejčastějším způsobem získávání cenných dat a šíření malwaru. Nedávné statistiky ukazují, že více než polovina (53,2 %) kriminálních aktivit na internetu je spojena s touto kybernetickou kriminalitou. Každý den je odesláno přibližně 3,4 miliardy nevyžádaných e-mailů. Díky technologickému pokroku se phishing stal dostupnějším a účinnějším, často ve spojení s útoky ransomwaru. Ačkoli phishing prostřednictvím e-mailu představuje stálou hrozbu již od počátků internetu, hackeři vyvinuli specializované verze phishingu přizpůsobené různým komunikačním kanálům. Například spear phishing se zaměřuje na konkrétní skupiny ve firmě a k oklamání potenciálních obětí používá sofistikovanější terminologii. Naproti tomu whaling se zaměřuje na vysoce postavené vedoucí pracovníky, jako je například vedení společnosti. V úvodním čtvrtletí roku 2023 bylo téměř 60 % e-mailů nahlášených zaměstnanci zaměřeno na krádež přihlašovacích údajů.[139]

4.2 Mezinárodní spolupráce v kybernetické bezpečnosti

V době, kdy digitální útoky států a kybernetická kriminalita rychle překračují hranice států a přerůstají globální krize, se mezinárodní spolupráce stala naléhavou prioritou. Potřeba globální spolupráce při zvládání různých naléhavých hrozeb, od kybernetické špionáže až po útoky ransomwaru na kritickou infrastrukturu, je nezbytně nutná, aby se zabránilo hospodářským a sociálním katastrofám.[140]

Díky spolupráci mohou země kybernetické hrozby sledovat napříč hranicemi a získat tak

[138] A Year in Review: Cybersecurity Trends and Challenges in 2023," C8 Secure, 17. 11. 2023, https://www.c8secure.com/2023/11/17/a-year-in-review/ (staženo 10. 12. 2023).
[139] Ibidem.
[140] Cynthia Brumfield, International cooperation is key to fighting threat actors and cybercrime, CSO, 19. 9. 2022, https://www.csoonline.com/article/573649/international-cooperation-is-key-to-fighting-threat-actors-and-cybercrime.html (staženo 11. 12. 2023).

komplexní přehled o jejich původu a metodách. Tato globální perspektiva je zásadní pro vypracování účinných protiopatření a preventivních strategií. Mezinárodní spolupráce je v tomto kontextu nejen přínosná, ale i nezbytná pro důkladnou obranu proti kybernetickým hrozbám, které nerespektují státní hranice. Rozdíly ve schopnostech v oblasti kybernetické bezpečnosti mezi jednotlivými státy jsou značné - některé země jsou v oblasti technologií a postupů kybernetické bezpečnosti na špičce, zatímco jiné mohou zaostávat. Mezinárodní spolupráce umožňuje sdílet zdroje, odborné znalosti a osvědčené postupy - toto sdílení přináší prospěch všem zúčastněným stranám, neboť zvyšuje celkovou úroveň připravenosti a schopnost rychlé reakce. Boj proti kybernetické kriminalitě je příkladem potřeby mezinárodní spolupráce. Kybernetičtí zločinci často působí za hranicemi a využívají právních a jurisdikčních mezer. Mezinárodní spolupráce je pro orgány činné v trestním řízení zásadní, aby mohly tyto zločince stíhat, sdílet zpravodajské informace a účinně provádět společné operace. Tato spolupráce rovněž pomáhá harmonizovat právní přístupy ke kybernetické kriminalitě a zajišťuje, že zločinci nemohou využívat mezer v různých vnitrostátních právních předpisech.[141]

Nedorozumění nebo napětí mezi zeměmi může často vzniknout v důsledku problémů v oblasti kybernetické bezpečnosti. Společné úsilí v této oblasti posiluje důvěru a porozumění, snižuje potenciál konfliktů a podporuje mírumilovnější a kooperativnější globální prostředí kyberprostoru. Problémy kybernetické bezpečnosti mohou významně ovlivnit globální ekonomiku a mezinárodní vztahy. Efektivní mezinárodní spolupráce v oblasti kybernetické bezpečnosti pomáhá tyto dopady zmírnit a zachovat globální ekonomickou stabilitu a politické vztahy. Je nezbytná pro zachování integrity mezinárodního obchodu a komunikačních systémů, které jsou stále více závislé na digitální infrastruktuře.[142]

Dalším důležitým aspektem mezinárodní spolupráce je vývoj globálních standardů a protokolů kybernetické bezpečnosti. Tato standardizace umožňuje konzistentní a jednotný přístup ke kybernetické bezpečnosti, který je klíčový pro ochranu systémů na celém světě.

[141] James Andrew Lewis, "Creating Accountability for Global Cyber Norms," CSIS, 23. 2. 2022, https://www.csis.org/analysis/creating-accountability-global-cyber-norms (staženo 11. 12. 2023).
[142] Ravikumar Ramachandran, "Cybersecurity and its Critical Role in Global Economy," ISACA, 23. 1. 2019, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/cybersecurity-and-its-critical-role-in-global-economy (staženo 11. 12. 2023).

Zjednodušuje proces zabezpečení sítí a informací, protože tyto standardy poskytují jasný rámec, kterým se organizace a vlády mohou řídit. Ty nejdůležitější milníky, kterých se zatím podařilo dosáhnout, jsou nastíněny na dalších stranách práce.

Budapešťská úmluva o kybernetické kriminalitě z roku 2001 je první mezinárodní smlouvou zaměřenou na boj proti kybernetické kriminalitě. Vznikla v důsledku rostoucí potřeby soudržného mezinárodního právního rámce pro řešení narůstajícího problému trestných činů páchaných prostřednictvím počítačových sítí, přičemž bylo uznáno, že tradiční teritoriální zákony nejsou vzhledem k povaze internetu aplikovatelné. Tato úmluva poskytla komplexní přístup k řešení kybernetické kriminality prostřednictvím harmonizace vnitrostátních právních předpisů, zlepšení vyšetřovacích technik a posílení spolupráce mezi státy. Zaměřila se na trestné činy proti integritě a dostupnosti počítačových dat a systémů, trestné činy související s počítači a trestné činy související s autorským právem. Budapešťská úmluva však čelila kritice a omezením. Některé země, zejména Rusko a Čína, se k ní nepřipojily s odkazem na obavy o národní suverenitu a soukromí. Navzdory těmto problémům zůstává úmluva základním kamenem v boji proti počítačové kriminalitě a představuje precedens pro mezinárodní spolupráci v této oblasti.[143]

Snahu o smlouvy v kybernetické bezpečnosti projevily i mezinárodní organizace. Politika kybernetické obrany NATO z roku 2008 byla významným krokem Severoatlantické aliance, která uznala kybernetické hrozby jako novou sféru. Tato politika uznala, že kybernetické útoky mohou potenciálně ohrozit národní a euroatlantickou prosperitu, bezpečnost a stabilitu. Jejím cílem bylo chránit vlastní komunikační a informační systémy NATO s ohledem na jejich zásadní roli v operacích a misích NATO. Politika zdůrazňovala potřebu koordinovaného přístupu ke kybernetické obraně napříč členy NATO se zaměřením na prevenci, obranu, odolnost a obnovu po kybernetických útocích. Tento přístup byl považován za klíčový pro zachování operační účinnosti aliance. Kromě toho znamenal uznání měnící se povahy vedení války a bezpečnosti v digitálním věku ze strany NATO. Tato politika položila základy pro následné aktualizace a strategie v závislosti na vývoji kybernetických hrozeb. Zdůraznila význam kybernetické bezpečnosti v

[143] "Council of Europe, Convention on Cybercrime (Treaty No. 185)," Council of Europe, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (staženo 11. 12. 2023).

mezinárodním bezpečnostním diskurzu a vytvořila precedens pro další mezinárodní organizace a země, které ji následovaly.[144]

Evropská unie se rovněž chopila iniciativy a v roce 2013 vytvořila svou strategii kybernetické bezpečnosti. Tato strategie byla reakcí na rostoucí kybernetické hrozby a rostoucí závislost států EU na digitálních technologiích. Její cíle zahrnovaly zajištění vysoké společné úrovně bezpečnosti sítí a informací v celé Unii, posílení schopností a připravenosti v oblasti kybernetické bezpečnosti, zefektivnění spolupráce mezi zeměmi EU, podporu globálního otevřeného a bezpečného kyberprostoru a podporu dynamického a inovativního průmyslu a výzkumného prostředí v oblasti kybernetické bezpečnosti. Tato strategie uznala, že incidenty v oblasti kybernetické bezpečnosti mohou mít významný dopad na vnitřní trh a individuální práva občanů EU. Zdůraznila význam komplexních opatření a společného přístupu k ochraně kritických infrastruktur, zlepšení rychlosti reakce na incidenty a zvýšení odolnosti informačních systémů.[145]

Koordinace bezpečnostních strategií se ale neomezuje pouze regionálně. Globální fórum pro kybernetickou odbornost (GFCE) bylo založeno v roce 2015 s cílem řešit rostoucí výzvy v oblasti kybernetické bezpečnosti na celém světě. Slouží jako globální platforma pro státy, mezinárodní organizace a subjekty ze soukromého sektoru, aby mohly spolupracovat a sdílet znalosti a osvědčené postupy v oblasti kybernetické bezpečnosti. Cílem GFCE je posílit kybernetickou odolnost, zejména v regionech s rozvíjejícími se kybernetickými schopnostmi, a to podporou budování kapacit, rozvoje politik a zaváděním praktických opatření v oblasti kybernetické bezpečnosti. K vytvoření fóra vedla potřeba společného a koordinovaného přístupu k účinnému zvládání komplexní a hranice překračující povahy kybernetických hrozeb a k posílení globální infrastruktury kybernetické bezpečnosti.[146]

Experti také tvrdí, že je nutné obnovení americko-ruského dialogu o kybernetických otázkách. Vztahy mezi Spojenými státy a Ruskem mají zásadní význam pro celý systém

[144] "Cyber deffence", NATO, naposledy upraveno 14. 11. 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm (staženo 11. 12. 2023).
[145] "The Cybersecurity Strategy", European Commision, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (staženo 11. 12. 2023).
[146] "The Global Forum on Cyber Expertise (GFCE)," The GFCE, https://thegfce.org/ (staženo 11. 12. 2023).

kybernetické politiky a diplomacie. Obě země patří k nejvyspělejším kybernetickým mocnostem a jako první vypracovaly opatření na budování důvěry v oblasti informačních a komunikačních technologií ("pakt o neútočení v kyberprostoru") a zůstávají v čele diskusí o globální kybernetické politice. Spory a vzájemné obviňování se mezi Spojenými státy a Ruskem se stupňují již několik let a jsou částečně příčinou pomalého pokroku při vytváření pravidel pro zodpovědné chování států v kybernetickém prostoru. Spojené státy se připojily ke skupině zemí, které trvají na tom, aby se stávající mezinárodní právo plně vztahovalo na kyberprostor, zatímco Rusko chce vytvořit novou smlouvu přizpůsobenou speciálně této oblasti. Dokud se budou obě strany ubírat takto různými směry, nelze v oblasti kybernetických norem dosáhnout žádného významného pokroku. Otázkou ale je, zda dialog mezi oběma stranami je vůbec možný, vzhledem k obviněním, že Rusko použilo informační a komunikační technologie k vměšování se do amerických prezidentských voleb v roce 2016 a že Spojené státy použily informační a komunikační technologie pro své vlastní geopolitické cíle, jak odhalil Edward Snowden.[147]

V podobné situaci se Spojené státy ocitly i v roce 2015, kdy byla administrativa Baracka Obamy blízko uvalení rozsáhlých sankcí proti Číně jako odplaty za to, že hackeři (údajně podporovaní čínskou vládou) ukradli průmyslová tajemství, což stálo americkou ekonomiku škody v řádu miliard dolarů. Namísto přerušení dialogu o kybernetických otázkách však Obama a čínský prezident Si Ťin-pching dokázali podepsat významnou dohodu o kybernetické hospodářské špionáži, která výrazně omezila kybernetické útoky Číny na Spojené státy. Americko-čínská dohoda byla realistická a měla omezený rozsah, o což by měly usilovat i Spojené státy a Rusko. Obě mocnosti by například mohly usilovat o dohodu omezenou na prevenci nebezpečných vojenských aktivit v kyberprostoru, podobnou americko-sovětské dohodě o incidentech na moři z roku 1972.[148]

---

[147] "Russia, US launch cybersecurity dialogue, three rounds already held, says diplomat", Tass Russian News Agency, 28. 7. 2021, https://tass.com/politics/1320507?utm_source=cybersecurity-review.com&utm_medium=referral&utm_campaign=cybersecurity-review.com&utm_referrer=cybersecurity-review.com https://www.russiamatters.org/analysis/us-russian-contention-cyberspace-are-rules-road-necessary-or-possible (staženo 12. 12. 2023).
Zabierek, Lauren, Christie Lawrence, Miles Neumann, a Pavel Sharikov, "US-Russian Contention in Cyberspace: Are Rules of the Road Necessary or Possible?" Russia Matters, 10. 6. 2021, https://www.russiamatters.org/analysis/us-russian-contention-cyberspace-are-rules-road-necessary-or-possible (staženo 12. 12. 2023).

[148] Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later, Council on Foreign Relations", 28. 11. 2016, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later (staženo 13. 12. 2023).

V roce 2004 byla zřízena Skupina vládních expertů OSN pro vývoj v oblasti informací a telekomunikací v kontextu mezinárodní bezpečnosti (UN GGE), která měla vypracovat společný přístup k tomu, jak by se vlády měly chovat v kyberprostoru. Její zpráva z roku 2015 poskytla základ pro mezinárodně uznávaný vládní kodex chování v kyberprostoru. Zpráva z roku 2015 doporučila jedenáct základních, důležitých norem, včetně ustanovení, že státy by neměly vědomě umožnit, aby jejich území bylo využíváno k mezinárodně protiprávním kybernetickým činům; neměly by provádět nebo vědomě podporovat činnosti v oblasti informačních a komunikačních technologií, které záměrně poškozují kritickou infrastrukturu; a měly by usilovat o zabránění šíření škodlivých technologií. GGE OSN bohužel v červnu 2017 nedosáhla konsenzu ohledně nástupce zprávy z roku 2015. Skupina však nezanikla a stále existuje. Namísto snahy o rozšíření zprávy z roku 2015 by měla získat silnější oficiální status, například v podobě rezoluce Valného shromáždění OSN. Pokud by byli jejími spoluautory všichni stálí členové Rady bezpečnosti OSN, pravděpodobně by získala širokou podporu dalších zemí. Přestože by rezoluce OSN nebyla závazná, posloužila by jako krok k institucionalizaci kybernetických norem.[149]

V rámci aktualizovaného rámce Atlantické charty se Spojené království a USA dohodly na bližším rozvoji partnerství v oblasti vědy a technologií. Toto partnerství má za cíl podnítit spolupráci v oblastech, jako je výzkum, inovace, komercializace, obrana, bezpečnost, prosazování práva a zpravodajství. Jeho cílem je rovněž zakotvit hodnoty liberálních demokracií a otevřených trhů.[150]

I Spojené státy a Spojené království mají mezi sebou uzavřenou dlouhodobou dohodu o posílení spolupráce v oblasti kybernetické bezpečnosti. Ta zahrnuje zvýšení kybernetického zabezpečení kritické infrastruktury, posílení sdílení informací o hrozbách a zpravodajské spolupráce a podporu vzdělávacích výměn mezi vědci a výzkumníky v

Farley, Robert, "Did the Obama-Xi Cyber Agreement Work?", The Diplomat, 11. 8. 2018, https://thediplomat.com/2018/08/did-the-obama-xi-cyber-agreement-work/ (staženo 13. 12. 2023).

[149] "2015 UN GGE - Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174)", Digital Watch Observatory, červenec 2015, https://dig.watch/resource/un-gge-report-2015-a70174 (staženo 13. 12. 2023).

[150] "UK and US agree to strengthen ties in science and technology", GOV.UK, 10. 6. 2021, https://www.gov.uk/government/news/uk-and-us-agree-to-strengthen-ties-in-science-and-technology (staženo 13. 12. 2023).

oblasti kybernetické bezpečnosti. Probíhají společná cvičení v oblasti kybernetické bezpečnosti a síťové obrany s cílem zlepšit kombinované reakce na kybernetické hrozby. Součástí partnerství je rovněž vytvoření společné kybernetické buňky GCHQ, MI5, NSA a FBI, která se zaměřuje na konkrétní témata kybernetické obrany a umožňuje rychlejší a rozsáhlejší sdílení informací a údajů o kybernetických hrozbách.[151]

Rovněž spolu aktivně vedou dialog o nových technologiích a důležitých datech. Tato iniciativa navazuje na závazek z roku 2021 rozvíjet dvoustranné technologické partnerství. Cílem dialogu je řešit společné priority v oblasti technologií, včetně přeshraničních datových toků, diverzifikace telekomunikačního dodavatelského řetězce, umělé inteligence a kvantových informačních věd. Tato spolupráce podtrhuje strategický význam technologií pro zajištění prosperity, bezpečnosti a prosazování demokratických hodnot v celosvětovém měřítku.[152]

I armády Spojeného království a Spojených států navázaly partnerství v boji proti kybernetickým hrozbám. Tato spolupráce zahrnuje strategické velitelství Spojeného království a kybernetické velitelství USA a zaměřuje se na identifikaci hrozeb, které by mohly ovlivnit vnitřní systémy jednoho ze států. Cílem partnerství je sjednotit reakce na škodlivé kybernetické aktivity a sdílet poznatky s cílem posílit kybernetickou odolnost.[153]

[151] "FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation." The White House, 16. 1. 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation (staženo 14. 12. 2023).
[152] "UK-US Joint Statement: New Comprehensive Dialogue on Technology and Data and Progress on Data Adequacy", GOV.UK, 7. 10. 2022, https://www.gov.uk/government/publications/uk-and-us-progress-tech-and-data-partnership/uk-us-joint-statement-new-comprehensive-dialogue-on-technology-and-data-and-progress-on-data-adequacy (staženo 14. 12. 2023).
[153] "The joint UK and US military partnership to combat cyberthreats", Open Access Government, 26. 10. 2022, https://www.openaccessgovernment.org/the-joint-uk-and-us-military-partnership-to-combat-cyberthreats/146506/ (staženo 14. 12. 2023).

Závěr

Jak Spojené státy, tak Spojené království si uvědomují potřebu chránit své informační systémy a s nimi související citlivá data, zejména ty, které jsou spojeny s vládou a kritickou infrastrukturou. Ačkoli se způsoby, kterými se toho snaží dosáhnout místy liší, především co do institucí, které jsou pověřené reakcemi na kybernetické incidenty, jejich cíle se shodují.

Tato práce podrobněji představuje reakci obou států na dosud největší kybernetické incidenty, které postihly jak Spojené státy, tak i Spojené království. Těmito incidenty jsou útok ransomwaru WannaCry v roce 2017, malwaru NotPetya rovněž v roce 2017, případ kybernetické špionáže, který proběhl na serveru SolarWinds v roce 2020 a státem sponzorovaný kybernetický útok na servery Microsoft Exchange v roce 2021. Na všechny tyto incidenty odpověděly oba státy pomocí jejich ústředního přístupu v oblasti kybernetické bezpečnosti, který je znám jako cyber deterrance. Avšak přístup cyber deterrance se potýká s významnými problémy, které omezují jeho účinnost. Hlavním problémem jsou obtíže s přiřazením zodpovědnosti za kybernetické útoky, které vzhledem k často anonymní povaze těchto hrozeb ztěžují možnost účinného odstrašení nebo odvety. Ačkoli se již zmíněné kybernetické útoky podařilo zastavit, státy se při nich ocitly spíše v pasivní pozici, kdy se soustředily na minimalizaci škod a aktéry útoků se nepodařilo účinně sankcionovat. Analýza jednotlivých případů nám také ukázala, že v každém z nich hrála klíčovou roli spolupráce mezi státy. Lze tedy přepokládat, že pro posílení kybernetické bezpečosti států je naprosto klíčové sjednání mezinárodních norem a pravidel a posílení jejich spolupráce.

Práce prostřednictvím konkrétních případů poukázala na to, že přílišné spoléhání se pouze na kybernetické odstrašování může vyvolat falešný pocit bezpečí, což by mohlo zastínit význam rozvoje komplexních obranných opatření. Úskalím cyber detterence je i to, že by tato strategie mohla vést k použití prostředků, které jsou na hraně jak právní, tak i etické, jako je například použití útočných kybernetických sil, které by mohly poškodit třetí strany nebo zbytečně eskalovat konflikt. Ačkoli má tedy kybernetické odstrašování ve strategii kybernetické bezpečnosti rozhodně své místo, jeho limitace zdůrazňují potřebu vyváženějšího přístupu, který vedle případných odstrašujících opatření zdůrazňuje nutnost

vybudovat i obranné schopnosti a pro případ nejhoršího posílit i ty ofensivní.

Summary

Both the United States and the United Kingdom recognize the need to protect their information systems and sensitive data, especially those associated with government and critical infrastructure. Although the ways in which they seek to do this differ in places, particularly in terms of the institutions charged with responding to cyber incidents, their goals are the same.

This paper details the responses of both countries to the largest cyber incidents to date, which have affected both the United States and the United Kingdom. These incidents include the WannaCry ransomware attack in 2017, the NotPetya malware attack also in 2017, the cyber espionage case that took place on the SolarWinds server in 2020, and the state-sponsored cyber attack on Microsoft Exchange servers in 2021. Both states responded to all of these incidents using their central cybersecurity approach known as cyber deterrence. However, the cyber deterrance approach faces significant challenges that limit its effectiveness. The main problem is the difficulty in assigning responsibility for cyber attacks, which, given the often anonymous nature of these threats, makes it difficult to effectively deter or retaliate. Although the aforementioned cyber-attacks have been stopped, they have left states in a rather passive position, focusing on minimising the damage and failing to effectively sanction the perpetrators. The analysis of the individual cases also showed that cooperation between states played a key role in each case. Thus, it can be assumed that negotiating international norms and rules and strengthening cooperation between states is absolutely crucial for strengthening their cybersecurity.

As demonstrated on the specific cases, over-reliance on cyber deterrence alone can create a false sense of security, which could obscure the importance of developing comprehensive defence measures. Relying heavily on deterrence might lead to actions that raise legal and ethical concerns, such as the use of offensive cyber capabilities that could inadvertently harm innocent third parties or escalate to unintended levels of conflict. Thus, while cyber deterrence certainly has its place in a cybersecurity strategy, its limitations highlight the need for a more balanced approach that emphasises the need to build defensive capabilities alongside potential deterrence measures and to strengthen offensive ones in case of the worst.

Použitá literatura

Adam Segal. " The U.S.-China Cyber Espionage Deal One Year Later. Council on Foreign Relations". 28. 11. 2016. https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later (staženo 13. 12. 2023).

Alberts. D.- Garstka . J.- Stein. F. Network Centric Warfare. 2. vyd. . Washington: CCRP . 2000. 284 s. ISBN 1-57906-019-6

Ann Barron-DiCamillo . "Written testimony of NPPD for a House Committee on Oversight and Government Reform hearing titled 'Examining ObamaCare's Failures in Security . Accountability . and Transparency'." Department of Homeland Security . 18. 9. 2014 . https://www.dhs.gov/news/2014/09/18/writte-testimony-nppd-house-committee-oversight-and-government-reform-hearing. (staženo 20. 9. 2023).

Bastl . Martin . Gruberová . Zuzana . Kyberprostor jako „pátá doména"? . Vojenské rozhledy . 2013 . roč. 22 (54) . č. 4 . s. 10-21 . ISSN 1210-3292 . www.vojenskerozhledy.cz (staženo 3. 5. 2023).

Bill Goodwin. "National Cyber Force carrying out daily hacking operations to disrupt hostile threats ." Computer Weekly . 4. 4. 2023 . https://www.computerweekly.com/news/365534733/National-Cyber-Force-carrying-out-daily-hacking-operations-to-disrupt-hostile-threats (staženo 7. 11. 2023).

Bílý dům 2011. UK Cabinet Office 2011

Blank . S 2008 . 'Web war I: is Europe's first information war a new kind of war?' . Comparative Strategy . vol. 27 . no. 3 . str. 227-47.

C8 Secure . "A Year in Review: Cybersecurity Trends and Challenges in 2023." 17. 11. 2023. https://www.c8secure.com/2023/11/17/a-year-in-review/ (staženo 9. 12. 2023).

Cabinet Office. "Cyber Security Strategy of the United Kingdom safety . security and resilience in cyber space". June 2009. Cyber Security Strategy of the United Kingdom safety . security and resilience in cyber space CM 7642 (publishing.service.gov.uk) str. 12 . (staženo 11. 10. 2023).

Cabinet Office. "The UK Cybersecurity Strategy". duben 2016 . https://assets.publishing.service.gov.uk/media/5a81bae5e5274a2e8ab558ca/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (staženo 11. 5. 2023).

Caton . Jeffrey L. And J. Boone Bartholomees. "On The Theory Of Cyberspace." Volume I: Theory Of War And Strategy . Strategic Studies Institute . US Army War College . 2012 .

str. 325–44. JSTOR . Http://Www.Jstor.Org/Stable/Resrep12116.26 (staženo 5. 5. 2023).
Center for Internet Security (CIS). "The SolarWinds Cyber-Attack: What You Need to Know." 15. 3. 2021 . https://www.cisecurity.org/solarwinds (staženo 27. 11. 2023).
Center for Strategic and International Studies ."Net Losses: Estimating the Global Cost of Cybercrime." 5. 6. 2014. https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime (staženo 11. 5. 2023).
CISecurity.org. "Ransomware: The Data Exfiltration and Double Extortion Trends". https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (staženo 10. 12. 2023).
Conrad Prince. " On the Offensive: The UK's New Cyber Force ." Royal United Services Institute. 23. 11. 2020. https://www.rusi.org/explore-our-research/publications/commentary/offensive-uks-new-cyber-force (staženo 19. 11. 2023).
Conrad Prince CB. "On the Offensive: The UK's New Cyber Force ." Royal United Services Institute. November 23 . 2020 . https://www.rusi.org/explore-our-research/publications/commentary/offensive-uks-new-cyber-force (staženo 25. 10. 2023).
Council of Europe. "Council of Europe. Convention on Cybercrime (Treaty No. 185)." https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (staženo 11. 12. 2023).
Crosston . M 2011. "World gone cyber MAD: how mutually assured debilitation is the best hope for cyber deterrence". Strategic Studies Quarterly . vol. 5. no. 1. str. 100-16.
Cybersecurity & Infrastructure Security Agency . "Cybersecurity Information Sharing Act of 2015 Procedures and Guidance". Naposledy upraveno 15. října 2021. https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance (staženo 2. 10. 2023).
Cybersecurity & Infrastructure Security Agency . "Executive Order 13636 and Presidential Policy Directive 21. CISA. https://www.cisa.gov/executive-order-13636-and-presidential-policy-directive-21. (staženo 30. 9. 2023).
Cybersecurity & Infrastructure Security Agency . "Indicators Associated With WannaCry Ransomware . naposledy upraveno 6. 7. 2018. https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware (staženo 25. 11. 2023).
Cybersecurity and Infrastructure Security Agency . "CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products ." 13. 12.

2020 . https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network (staženo 30. 11. 2023).

Cybersecurity and Infrastructure Security Agency ." Cybersecurity & Infrastructure Security Agency". last revised November 20 . 2018 . https://www.cisa.gov/news-events/alerts/2018/11/19/cybersecurity-and-infrastructure-security-agency (staženo 20. 9. 2023).

Cybersecurity and Infrastructure Security Agency. "Supply Chain Compromise ." 7. 1. 2021. https://www.cisa.gov/news-events/alerts/2021/01/07/supply-chain-compromise (staženo 30. 11. 2023).

Cybersecurity: Deterrence Policy . Congressional Research Service . 18. 1. 2022 . https://crsreports.congress.gov/product/pdf/R/R47011#:~:text=Generally%2C%20cyberspace%20deterrence%20strategies%20seek .a%20low%20rate%20of%20success str. 1

Cynthia Brumfield . International cooperation is key to fighting threat actors and cybercrime . CSO . 19. 9. 2022 . https://www.csoonline.com/article/573649/international-cooperation-is-key-to-fighting-threat-actors-and-cybercrime.html (staženo 11. 12. 2023).

Danny Steed . "Evaluating the National Cyber Force's 'Responsible Cyber Power in Practice' ." Royal United Services Institute . 9. 2. 2021 . https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice (staženo 10. 11. 2023).

Danny Steed . "The National Cyber Force: directions and implications for the UK ." Elcano Royal Institute . February 9 . 2021 . https://www.realinstitutoelcano.org/en/analyses/the-national-cyber-force-directions-and-implications-for-the-uk/ (staženo 10. 11. 2023).

David Burg a Sean Joyce . "Cybersecurity after WannaCry: How to Resist Future Attacks ." Strategy+Business . 16. 5. 2017 . https://www.strategy-business.com/blog/Cybersecurity-After-WannaCry-How-to-Resist-Future-Attacks (staženo 25. 11. 2023).

Department of Health and Social Care . "Government Sets Out Strategy to Protect NHS from Cyber Attacks ."naposledy upraveno 12. 6. 2021 . https://www.gov.uk/government/news/government-sets-out-strategy-to-protect-nhs-from-cyber-attacks (staženo 2. 12. 2023).

Department of Homeland Security . "DHS Statement on Ongoing Ransomware Attacks ." 12. 5. 2017 . https://www.dhs.gov/news/2017/05/12/dhs-statement-ongoing-ransomware-attacks (staženo 25. 11. 2023).

Diego Laje and Nuray Taylor . "U.S. To Increase Cyber Capabilities . Research and Funding

with NATO ." AFCEA International . 29. 6. 2022 . https://www.afcea.org/signal-media/us-increase-cyber-capabilities-research-and-funding-nato (staženo 25. 11. 2023).

Digital Medicine 2 . no. 98 (2019).“A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.” https://doi.org/10.1038/s41746-019-0161-6 (staženo 2. 12. 2023).

Digital Watch Observatory . "2015 UN GGE - Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174)" . červenec 2015 . https://dig.watch/resource/un-gge-report-2015-a70174 (staženo 13. 12. 2023).

Dobbins . James . et al. “Cybersecurity.” Choices for America in a Turbulent World: Strategic Rethink . RAND Corporation . 2015 . str. 57–68. JSTOR . http://www.jstor.org/stable/10.7249/j.ctt17mvhfj

Emma Kohse and Chris Mirasola . "To Split or Not to Split: The Future of CYBERCOM’s Relationship with NSA ." Lawfare . 12. 4. 2017 . https://www.lawfaremedia.org/article/split-or-not-split-future-cybercoms-relationship-nsa (staženo 4. 10. 2023).

Erica D. Lonergan . "Defend Forward: Adapting Offense and Defense Strategy to Cyberspace ." Yale Cyber Leadership Forum . 20. 6. 2021 . https://www.cyber.forum.yale.edu/blog/2021/7/20/defend-forward-adapting-offense-and-defense-strategy-to-cyberspace (staženo 10. 11. 2023).

European Commision. “The Cybersecurity Strategy“ . https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (staženo 11. 12. 2023).

Farley . Robert. "Did the Obama-Xi Cyber Agreement Work?" . The Diplomat . 11. 8. 2018 . https://thediplomat.com/2018/08/did-the-obama-xi-cyber-agreement-work/ (staženo 13. 12. 2023).

Federal Bureau of Investigation . "Foreign Intelligence Surveillance Act (FISA) and Section 702." FBI. https://www.fbi.gov/investigate/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702 (staženo 3. 11. 2023).

Federal Information Security Modernization Act. "Cybersecurity & Infrastructure Security Agency“. 'https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act. (staženo 17. 9. 2023).

Federation of American Scientists. "Presidential Decision Directive/NSC-63 ." 22. 5. 1998 . https://irp.fas.org/offdocs/pdd/pdd-63.htm (staženo 30. 9. 2023).

Ferrillo . Paul. "The Importance of a Battle-Tested Cyber Incident Response Plan." Harvard Law School Forum on Corporate Governance . December 19 . 2014.

https://corpgov.law.harvard.edu/2014/12/19/the-importance-of-a-battle-tested-cyber-incident-response-plan/ (staženo 10. 5. 2023).

FinCEN. "Financial Action Task Force.". https://www.fincen.gov/resources/international/financial-action-task-force (staženo 11. 5. 2023).

Fisher Phillips. "The Use of Bitcoin and Cryptocurrencies in Ransomware Attacks: Why Employers Should Care". https://www.fisherphillips.com/en/news-insights/bitcoin-and-cryptocurrencies-ransomware-attacks.html (staženo 9. 12. 2023).

Foreign & Commonwealth Office a Lord (Tariq) Ahmad of Wimbledon. "Foreign Office Minister Condemns Russia for NotPetya Attacks ." naposledy upraveno 15. 2. 2018 . https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (staženo 2. 12. 2023).

Fourth Edition . Global Investigations Review. "Practical Issues in Cyber-Related Sanctions ." in The Guide to Sanctions . 29. 11. 2023 . https://globalinvestigationsreview.com/guide/the-guide-sanctions/fourth-edition/article/practical-issues-in-cyber-related-sanctions (staženo 21. 11. 2023).

Francis Maude. "Cyber Security Information Sharing Programme". GOV.UK . March 27 . 2013 . https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme (staženo 20. 10. 2023).

GOV.UK. "UK-US Joint Statement: New Comprehensive Dialogue on Technology and Data and Progress on Data Adequacy". 7. 10. 2022 . https://www.gov.uk/government/publications/uk-and-us-progress-tech-and-data-partnership/uk-us-joint-statement-new-comprehensive-dialogue-on-technology-and-data-and-progress-on-data-adequacy (staženo 14. 12. 2023).

GOV.UK. "Cabinet Office and The Rt Hon Lord Maude of Horsham . 'Government launches information sharing partnership on cyber security .' March 27 . 2013 . https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security (staženo 8. 10. 2023).

GOV.UK. "Government Digital Service . Cyber skills for a vibrant and secure UK." 12. 12. 2014. https://www.gov.uk/government/news/cyber-skills-for-a-vibrant-and-secure-uk (staženo 2. 12. 2023).

GOV.UK. "Permanent location of National Cyber Force campus announced ." October 3 . 2021 . naposledy upraveno 4. 10. 2021 . https://www.gov.uk/government/news/permanent-

location-of-national-cyber-force-campus-announced (staženo 25. 10. 2023).
GOV.UK. "Responsible Cyber Power in Practice ." 4. 4. 2023 . https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html (staženo 6. 11. 2023).
GOV.UK. "Telecommunications (Security) Bill ." naposledy upraveno 15. 1. 2021 . https://www.gov.uk/government/collections/telecommunications-security-bill (staženo 29. 10. 2023).
GOV.UK. "The Rt Hon George Osborne . 'Chancellor's speech to GCHQ on cyber security". November 17 . 2015 . https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security (staženo 25. 10. 2023).
GOV.UK. "UK and US agree to strengthen ties in science and technology". 10. 6. 2021 . https://www.gov.uk/government/news/uk-and-us-agree-to-strengthen-ties-in-science-and-technology (staženo 13. 12. 2023).
Government of the United Kingdom. "UK and Allies Hold Chinese State Responsible for a Pervasive Pattern of Hacking ." naposledy upraveno 19. 6. 2021 . https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking (staženo 7. 12. 2023).
Greiman . VA. “Cybersecurity And Global Governance.” Journal Of Information Warfare 14 . No. 4 (2015): 1–14. Https://Www.Jstor.Org/Stable/26487502.
Harriet Moynihan . "The Application of Sovereignty in Cyberspace ." Chatham House . 2. 12. 2019 . https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace (staženo 15. 11. 2023).
Charles H. Romine . "Bolstering Government Cybersecurity: Lessons Learned from WannaCry ." testimony before the Committee on Science . Space . and Technology . U.S. House of Representatives . 15. 6. 2017 . https://www.nist.gov/speech-testimony/bolstering-government-cybersecurity-lessons-learned-wannacry (staženo 25. 11. 2023).
Chris Ensor . "GCHQ . the National Technical Authority for Information Assurance ." Government security blog . August 11 . 2014 . https://securityprofession.blog.gov.uk/2014/08/11/gchq-the-national-technical-authority-for-information-assurance/ (staženo 8. 10. 2023).
Chris Jaikaran . "Cybersecurity: Deterrence Policy ." Congressional Research Service . R47011 . 18. 1. 2022 . https://www.everycrsreport.com/reports/R47011.html (staženo 23. 11. 2023).

International Cyber Law: Interactive Toolkit. "Operation Glowing Symphony (2016) ." naposledy upraveno 4. 6. 2021 . https://cyberlaw.ccdcoe.org/wiki/Operation_Glowing_Symphony_(2016) (staženo 4. 10. 2023).

ISC2.org. "ISC2 . 'ISC2 Reveals Workforce Growth But Record-Breaking Gap: 4 Million Cybersecurity Professionals". 23. 10. 2023 . https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals (staženo 9. 12. 2023).

Jack Freund . "Understanding the Distinction Between Cyberwar and Espionage ." ISACA . April 27 . 2022 . https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-17/understanding-the-distinction-between-cyberwar-and-espionage (staženo 29. 10. 2023).

Jadyn Marks . "Gabbard's Espionage Act Reform Bill Highlights U.S. Government's Recent Responses to National Security Whistleblowers ." American Bar Association . January 31. 2021.https://www.americanbar.org/groups/crsj/publications/crsj-featured-articles/espionage-act-reform-bill/ (staženo 29. 10. 2023).

Jake Harrington and Riley McCabe . "The Case for Cooperation: The Future of the U.S.-UK Intelligence Alliance ." CSIS. 15. 3. 2022 . https://www.csis.org/analysis/case-cooperation-future-us-uk-intelligence-alliance (staženo 19. 11. 2023).

James A. Lewis. "Cyber Security and the Intelligence Community ." Belfer Center for Science and International Affairs . last modified December 15. 2021. https://www.belfercenter.org/publication/cyber-security-and-intelligence-community (staženo 5. 11. 2023).

James Andrew Lewis . "Creating Accountability for Global Cyber Norms ." CSIS . 23. 2. 2022 . https://www.csis.org/analysis/creating-accountability-global-cyber-norms (staženo 11. 12. 2023).

James Andrew Lewis . "Deterrence and Cyber Strategy ." CSIS . 15. 11. 2023 . https://www.csis.org/analysis/deterrence-and-cyber-strategy (staženo 21. 11. 2023).

James Andrew Lewis . "The Rationale for Offensive Cyber Capabilities ." Strategic Technologies Blog . CSIS . last modified July 13 . 2021 . https://www.csis.org/blogs/strategic-technologies-blog/rationale-offensive-cyber-capabilities (staženo 5. 11. 2023).

James Olthoff . "Setting the Standards: Strengthening U.S. Leadership in Technical

Standards ." National Institute of Standards and Technology . 17. 3. 2022 . https://www.nist.gov/speech-testimony/setting-standards-strengthening-us-leadership-technical-standards (staženo 17. 9. 2023).

Jamie MacColl . "The UK's Approach to Russian Cyber Operations Shows No Signs of Changing ." Royal United Services Institute . 21. 5. 2021 . https://www.rusi.org/explore-our-research/publications/commentary/uks-approach-russian-cyber-operations-shows-no-signs-changing (staženo 7. 12. 2023).

Jason Bartlett and Megan Ophel . "Sanctions by the Numbers: Spotlight on Cyber Sanctions ." Center for a New American Security . 4. 5. 2021 . https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber (staženo 19. 11. 2023).

Jason Lau . "State of Cybersecurity 2023: Navigating Current and Emerging Threats ." ISACA . 2. 8. 2023 . https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/state-of-cybersecurity-2023-navigating-current-and-emerging-threats (staženo 24. 11. 2023).

Jeremy Hunt . "Deterrence in the Cyber Age ." speech delivered at Glasgow University . 7. 3. 2019 . UK Government . https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary (staženo 21. 11. 2023).

Jessica Davis . "DOJ Indicts Russian Hackers Behind 2017 NotPetya Malware Attack ." HealthITSecurity . 20 8. 2020 . https://www.healthitsecurity.com/news/doj-indicts-russian-hackers-behind-2017-notpetya-malware-attack/ (staženo 27. 11. 2023).

John Oates . "UK.gov decides best form of cyber defence is attack" . The Register . June 25 . 2009 . https://www.theregister.com/2009/06/25/uk_cyber_security_strategy/ (staženo 11. 10. 2023).

Josh Fruhlinger . "Stuxnet explained: The first known cyberweapon" . CSO . 31. 8. 2022 . https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html (staženo 11. 5. 2023).

Klimburg . A. 2011 . 'Mobilizing cyber power' . Survival . vol. 53 . no. 1 . str. 41-60.

Korns . S & Kastenberg . J 2009 . 'Georgia's cyber left hook' . Parameters . vol. 38 . no. 4 . str. 60-76.

Kristan Stoddart . "UK cyber security and critical national infrastructure protection" . International Affairs . Volume 92 . Issue 5 . 31. 8. 2016 . strany 1079–1105 . https://academic.oup.com/ia/article-abstract/92/5/1079/2688134?redirectedFrom=fulltext

(staženo 2. 12. 2023).
Lawfare . "Everything You Know About the Vulnerability Equities Process Is Wrong ." https://www.lawfaremedia.org/article/everything-you-know-about-vulnerability-equities-process-wrong (staženo 3. 11. 2023).
legislation.gov.uk. "Intelligence Services Act 1994 ." https://www.legislation.gov.uk/ukpga/1994/13/contents (staženo 3. 11. 2023).
legislation.gov.uk. "Telecommunications (Security) Act 2021 ." November 17 . 2021 . https://www.legislation.gov.uk/ukpga/2021/31/enacted (staženo 29. 10. 2023).
Marcus H. Sachs . "Reflections on Executive Order 13010 ." McCrary Institute . 15. 7. 2021 . https://mccrary.auburn.edu/work/insights/reflections-on-executive-order-13010/ (staženo 21. 9. 2023).
Mark Pomerleau . "Cyber Command granted new . expanded authorities ." C4ISRNET . 28. 2. 2018 . https://www.c4isrnet.com/dod/cybercom/2018/02/28/cyber-command-granted-new-and-expanded-authorities/ (staženo 8. 10. 2023).
Mark Pomerleau . "New authorities mean lots of new missions at Cyber Command ." C4ISRNet . 8. 5. 2019 . https://www.c4isrnet.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/ (staženo 13. 11. 2023).
Mark Say . "NCSC Publishes Guidance on Responses to Cyber Attacks ." UKAuthority . naposledy upraveno 2. 11. 2020 . https://www.ukauthority.com/articles/ncsc-publishes-guidance-on-responses-to-cyber-attacks/ (staženo 5. 12. 2023).
Mark Spangler . "Offensive Cyber Operations: A National Security Imperative ." AFCEA International . 29. 6. 2023 . https://www.afcea.org/signal-media/cyber-edge/offensive-cyber-operations-national-security-imperative (staženo 23. 11. 2023).
Martin Libicki . Cyberdeterrence and Cyberwar . Santa Monica . Calif.: RAND Corporation . MG-877 . 2009 . str. 112.
Max Smeets . "Cyber Command's Strategy Risks Friction With Allies ." Lawfare . 28. 5. 2019 . https://www.lawfaremedia.org/article/cyber-commands-strategy-risks-friction-allies (staženo 10. 11. 2023).
Mayer Brown, Lexology. "The U.S. National Defense Authorization Act for Fiscal Year 2021: Cybersecurity Provisions". https://www.lexology.com/library/detail.aspx?g=b3332196-151c-4ae0-a800-bdc17e67d6e9#:~:text=Section%201705%20authorizes%20CISA%20to .vulnerabilities%20within%20Federal%20information (staženo 20. 9. 2023).

Michael Hardy. "The wake-up call ." Federal Times . 11. 7. 2016 . https://www.federaltimes.com/smr/critical-infrastructure/2016/07/11/the-wake-up-call/ (staženo 20. 9. 2023).

Michael Martelle . "Eligible Receiver 97: Seminal DOD Cyber Exercise Included Mock Terror Strikes and Hostage Simulations ." National Security Archive . 1. 8. 2018 . https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations staženo (15. 9. 2023).

Michael Martelle. "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY ." National Security Archive . 21. 1. 2020 . https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony (staženo 6. 10. 2023).

Michael Schmitt. "US Transparency Regarding International Law in Cyberspace ." Just Security . 15. 11. 2016 . https://www.justsecurity.org/34465/transparency-international-law-cyberspace/ (staženo 17. 11. 2023).

Mike Burns. Matthew McWhirt . Douglas Bienstock . Nick Bennett . a Juraj Sucik . "Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452 ." Mandiant Blog . 19. 1. 2021 . https://www.mandiant.com/resources/blog/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452 (staženo 30. 11. 2023).

Moteff . John D. “Critical Infrastructures: Background, Policy, and Implementation“. 10. 6. 2015. Congressional Research Service. https://sgp.fas.org/crs/homesec/RL30153.pdf str. 6 (staženo 17. 9. 2023).

National Audit Office (NAO). "Investigation: WannaCry cyber attack and the NHS". 27. 10. 2017. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/.https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/ (staženo 2. 12. 2023).

National Audit Office (NAO). "Progress of the 2016-2021 National Cyber Security Programme". 15. 3. 2019. https://www.nao.org.uk/press-releases/progress-of-the-2016-2021-national-cyber-security-programme/ (staženo 2. 12. 2023).

National Crime Agency . "Cyber Crime". https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime (staženo 2. 12. 2023).

National Cyber Security Centre. "Advice Following Microsoft Vulnerabilities Exploitation ." https://www.ncsc.gov.uk/news/advice-following-microsoft-vulnerabilities-exploitation

(staženo 7. 12. 2023).

National Cyber Security Centre . "NCSC Statement on SolarWinds Compromise ." . National Cyber Security Centre . "UK and US Call Out Russia for SolarWinds Compromise ." https://www.ncsc.gov.uk/news/ncsc-statement-on-solarwinds-compromise (staženo 5. 12. 2023).

National Cyber Security Centre . "Russian Military Almost Certainly Responsible for Destructive 2017 Cyber Attack" . naposledy upraveno 17. 2. 2018 . https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack (staženo 2. 12. 2023).

NATO. “Cyber deffence“ . naposledy upraveno 14. 11. 2023 . https://www.nato.int/cps/en/natohq/topics_78170.htm (staženo 11. 12. 2023).

NCSC . "National Cyber Security Centre . '2020 Annual Review ." 15. 3. 2021 . https://www.ncsc.gov.uk/annual-review/2020/index.html (staženo 1. 12. 2023).

Neil Ashdown . "UK and US Confirm Russian Responsibility for SolarWinds Attack ." Jane's Defence News . 6. 5. 2021 . https://www.janes.com/defence-news/news-detail/uk-and-us-confirm-russian-responsibility-for-solarwinds-attack (staženo 5. 12. 2023).

OECD. "Centre for the Protection of National Infrastructure (CPNI)" . https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/centrefortheprotectionofnationalinfrastructurecpni.htm#:~:text=CPNI%20was%20formed%20on%201 .NSAC (staženo 11. 10. 2023).

OODA Loop . "UK Blames China for Microsoft Exchange Server Hack ." OODA Loop . 19. 6. 2021 . https://www.oodaloop.com/briefs/2021/07/19/uk-blames-china-for-microsoft-exchange-server-hack/ (staženo 7. 12. 2023).

Open Access Government . "The joint UK and US military partnership to combat cyberthreats" . 26. 10. 2022 . https://www.openaccessgovernment.org/the-joint-uk-and-us-military-partnership-to-combat-cyberthreats/146506/ (staženo 14. 12. 2023).

Pendino . Stephanie LCDR . Jahn . Robert K. MAJ . Sr. . a Pedersen . Kirk Mr.„U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light." Joint Forces Staff College . September 7 . 2022. https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/ (staženo 10. 5. 2023).

Pieter Arntz . "US . EU . UK . NATO blame China for 'reckless' Exchange attacks ." Malwarebytes . 20. 6. 2021 . https://www.malwarebytes.com/blog/news/2021/07/us-eu-uk-

nato-blame-china-for-reckless-exchange-attacks (staženo 24. 11. 2023).
Price . Sean K. "Perfidy in Cyberspace: The Requirement for Human Confidence." Harvard National Security Journal . February 21 . 2020. https://harvardnsj.org/2020/02/21/perfidy-in-cyberspace-the-requirement-for-human-confidence/ (staženo 10. 5. 2023).
Ravikumar Ramachandran . "Cybersecurity and its Critical Role in Global Economy ." ISACA . 23. 1. 2019 . https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/cybersecurity-and-its-critical-role-in-global-economy (staženo 11. 12. 2023).
Robert Hannigan . "Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre ." Royal United Services Institute . February 27 . 2019 . https://www.rusi.org/explore-our-research/publications/occasional-papers/organising-government-cyber-creation-uks-national-cyber-security-centre (staženo 25. 10. 2023).
Robert Chesney . "The Domestic Legal Framework for U.S. Military Cyber Operations ." Lawfare . 5. 8. 2020 . https://www.lawfaremedia.org/article/domestic-legal-framework-us-military-cyber-operations (staženo 17. 11. 2023).
Robert Morgus . John Costello . Charles Garzoni . a Michael Garcia . "Deterrence by Denial: The Missing Element of U. S. Cyber Strategy ." Lawfare . 11. 3. 2020 . https://www.lawfaremedia.org/article/deterrence-denial-missing-element-us-cyber-strategy (staženo 21. 11. 2023).
Ronda Swaney . "Why Keep Cybercom and NSA's Dual-Hat Arrangement? ." Security Intelligence . 11. 9. 2023 . https://securityintelligence.com/articles/why-keep-cybercom-and-nsas-dual-hat-arrangement/ (staženo 6. 11. 2023).
S. Deputy Secretary of Defense Gordon England . "The Definition of 'Cyberspace' ." Memorandum for Secretaries of the Military Departments . Washington . DC . 12. 5. 2008 . integrator.hanscom.af.mil/2008/ May/05292008/05292008-24.htm (staženo 3. 5. 2023).
Saira Ghafur . Guy Martin . J. James Kinross . Chris Hankin . a Ara Darzi ."WannaCry—a Year On ." BMJ 361 (2018): k2381 . https://doi.org/10.1136/bmj.k2381 (staženo 2. 12. 2023).
Sam Ingalls . "FireEye . SolarWinds Breaches: Implications and Protections ." eSecurity Planet . 18. 12. 2020 . https://www.esecurityplanet.com/threats/fireeye-solarwinds-breaches-implications-protections/ (staženo 27. 11. 2023).
Sdělení č. 104/2013 Sb. m. s.; Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě dostupné z: 104/2013 Sb. m. s. Úmluva o počítačové kriminalitě (zakonyprolidi.cz) (staženo 10. 5. 2023).

Stephanie Pendino . Robert K. Jahn . Sr. . a Kirk Pedersen . "U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light ." Joint Forces Staff College . 7. 11. 2022 . https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/ (staženo 23. 11. 2023).

Stuart Littlewood . "Look Who's in Charge of UK Government Cyber Security ." Global Research . November 8 . 2015 . https://www.globalresearch.ca/look-whos-in-charge-of-uk-government-cyber-security/5487359 (staženo 25. 10. 2023).

Tass Russian News Agency .“Russia . US launch cybersecurity dialogue . three rounds already held . says diplomat“ . 28. 7. 2021 . https://tass.com/politics/1320507?utm_source=cybersecurity-review.com&utm_medium=referral&utm_campaign=cybersecurity-review.com&utm_referrer=cybersecurity-review.com

https://www.russiamatters.org/analysis/us-russian-contention-cyberspace-are-rules-road-necessary-or-possible (staženo 12. 12. 2023).

TechHQ . "Government-led Initiatives as Critical to National Cyber Defenses ." 19. 4. 2022 . https://techhq.com/2022/04/government-led-initiatives-as-critical-to-national-cyber-defenses/ (staženo 7. 11. 2023).

The 2011 UK Cybersecurity Strategy

The GFCE . "The Global Forum on Cyber Expertise (GFCE) ." https://thegfce.org/ (staženo 11. 12. 2023).

The UK Cyber Security Strategy 2011-2016: Annual Report. 14. 42016 . "Cabinet Office and National Security and Intelligence". https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report (staženo 20. 10. 2023).

The White House. "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government ." 14. 4. 2021 . https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (staženo 28. 11. 2023).

The White House. "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware ." 13. 10. 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ (staženo 25. 11. 2023).

The White House . "FACT SHEET: President Signs Executive Order Charting New Course

to Improve the Nation’s Cybersecurity and Protect Federal Government Networks ." 12. 5. 2021 . https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ (staženo 28. 11. 2023).

The White House . "FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation." 16. 1. 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation (staženo 14. 12. 2023).

The White House. "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China ." 19. 6. 2021 . https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/ (staženo 30. 11. 2023).

Tim Stevens . Rory Cormac . Erica D Lonergan . Dan Lomas . Dr. Pia Hüsch . and Joe Devanny . "Evaluating the National Cyber Force’s ‘Responsible Cyber Power in Practice’ ." Royal United Services Institute . 14. 4. 2023 . https://www.rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice (staženo 10. 11. 2023).

U.S. Cyber Command "CYBER 101 - Defend Forward and Persistent Engagement .". 25. 10. 2022 . https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/ (staženo 7. 11. 2023).

U.S. Cyber Command. "History of U.S. Cyber Command". https://www.cybercom.mil/About/History/. (staženo 15. 9. 2023).

U.S. Department of the Treasury. "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks ." 15. 3. 2018 . https://home.treasury.gov/news/press-releases/sm0312 (staženo 27. 11. 2023).

U.S. Government Accountability Office Blog. "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response". (infographic) 22. 4. 2021. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (staženo 30. 11. 2023).

U.S. Government Accountability Office. "Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents." GAO-22-104746 . 13. 1. 2022. https://www.gao.gov/products/gao-22-104746 (staženo 1. 12. 2023).

Uday Ali Pabrai . "US DoD Launches Comprehensive CMMC 2.0 Cybersecurity

Framework ." ISACA . 25. 1. 2022 . https://www.isaca.org/resources/news-and-trends/industry-news/2022/us-dod-launches-comprehensive-cmmc-2-cybersecurity-framework (staženo 2. 10. 2023).

UK Government . "Cabinet Office and Department for Business, Innovation & Skills . '2010 to 2015 Government Policy: Cyber Security". 8. 5. 2015. https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security (staženo 1. 12. 2023).

United Kingdom Government . "Application of international law to states' conduct in cyberspace: UK statement." 3. 6. 2021 . https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (staženo 17. 11. 2023).

United States Department of State. "Cybercrime." U.S. Department of State . https://www.state.gov/cybercrime (staženo 19. 11. 2023).

US Department of Defence. "Fact Sheet: 2023 DoD Cyber Strategy". May 2023. https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF#:~:text=2023%20DoD%20Cyber%20Strategy .It%20complements%20the (staženo 15. 9. 2023).

Venkina . Ekaterina. "How Denmark became the most cyber-secure country." IPS Journal . July 20 . 2021. https://www.ips-journal.eu/work-and-digitalisation/how-denmark-became-the-most-cyber-secure-country-5290/ (staženo 13. 9. 2023).

Viral Gandhi . "2023 ThreatLabz Report Indicates 400% Growth in IoT Malware Attacks ." Zscaler Blog . 24. 10. 2023 . https://www.zscaler.com/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks (staženo 9. 12. 2023).

VirtualArmour Team. "The Evolution of Cybersecurity in the UK vs. US.". VirtualArmour . 28. 2. 2017 . https://virtualarmour.com/the-evolution-of-cybersecurity-in-the-uk-vs-us/ (staženo 13. 9. 2023).

Wade H. Atkinson . Jr. . "A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy ." The Institute of World Politics . October 22 . 2020 . https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/ (staženo 2. 10. 2023).

Wolford . Ben. "What is GDPR . the EU’s new data protection law?" GDPR.eu. https://gdpr.eu/what-is-gdpr/ (staženo 10. 5. 2023).
Zabierek . Lauren. Christie Lawrence . Miles Neumann . a Pavel Sharikov . "US-Russian Contention in Cyberspace: Are Rules of the Road Necessary or Possible?" Russia Matters . 10. 6. 2021. https://www.russiamatters.org/analysis/us-russian-contention-cyberspace-are-rules-road-necessary-or-possible (staženo 12. 12. 2023).