ROZHODNUTÍ RADY (SZBP) 2020/1127

ze dne 30. července 2020,

kterým se mění rozhodnutí (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na článek 29 této smlouvy,

s ohledem na návrh vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku,

vzhledem k těmto důvodům:

(1) Dne 17. května 2019 přijala Rada rozhodnutí (SZBP) 2019/797 ([1]).

(2) Cílená omezující opatření proti kybernetickým útokům s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy, patří mezi opatření, která jsou součástí rámce Unie pro společnou diplomatickou reakci na nepřátelské činnosti v kyberprostoru (soubor nástrojů pro kybernetickou diplomacii), a jsou klíčovým nástrojem pro odrazování od těchto činností a reakci na ně. Omezující opatření lze uplatnit rovněž v reakci na kybernetické útoky s významným dopadem na třetí státy nebo mezinárodní organizace, je-li to považováno za nezbytné pro dosažení společných zahraničněpolitických a bezpečnostněpolitických cílů stanovených v relevantních ustanoveních článku 21 Smlouvy o Evropské unii.

(3) Dne 16. dubna 2018 přijala Rada závěry, v nichž důrazně odsoudila nepřátelské využívání informačních a komunikačních technologií, a to i v rámci kybernetických útoků veřejně známých pod názvem „WannaCry“ a „NotPetya“, které způsobily významné škody a ekonomické ztráty v Unii i mimo ni. Předsedové Evropské rady a Evropské komise a vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku vyjádřili dne 4. října 2018 v rámci společného prohlášení vážné znepokojení ohledně pokusu o kybernetický útok, jehož cílem bylo narušit integritu Organizace pro zákaz chemických zbraní (OPCW) v Nizozemsku a který byl agresivním aktem dokládajícím pohrdání důležitým posláním, které tato organizace plní. Vysoká představitelka v prohlášení jménem Unie ze dne 12. dubna 2019 naléhavě vyzvala příslušné aktéry, aby zastavili nepřátelské činnosti v kyberprostoru, jejichž cílem je oslabit celistvost, bezpečnost a hospodářskou konkurenceschopnost Unie, včetně vzrůstajícího počtu kybernetických krádeží duševního vlastnictví. Mezi tyto kybernetické krádeže patřily i krádeže provedené aktérem veřejně známým jako „APT10“ (Advanced Persistent Threat 10 – pokročilá trvalá hrozba 10).

(4) V této souvislosti a s cílem předcházet pokračujícím a stále intenzivnějším nepřátelským činnostem v kyberprostoru, odrazovat od nich a reagovat na ně by na seznam fyzických a právnických osob, subjektů a orgánů, na něž se vztahují omezující opatření, obsažený v příloze rozhodnutí (SZBP) 2019/797, mělo být zařazeno šest fyzických osob a tři subjekty či orgány. Tyto osoby, subjekty a orgány jsou odpovědné za kybernetické útoky nebo pokusy o ně, včetně pokusu o kybernetický útok na organizaci OPCW a kybernetické útoky veřejně známé jako „WannaCry“ a „NotPetya“, jakož i „operace Cloud Hopper“, nebo do těchto útoků byly zapojeny, podporovaly je nebo se jich účastnily.

(5) Rozhodnutí (SZBP) 2019/797 by proto mělo být odpovídajícím způsobem změněno,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Příloha rozhodnutí (SZBP) 2019/797 se mění v souladu s přílohou tohoto rozhodnutí.

([1]) Rozhodnutí Rady (SZBP) 2019/797 ze dne 17. května 2019 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 129 I, 17.5.2019, s. 13).

Článek 2

Toto rozhodnutí vstupuje v platnost dnem vyhlášení v *Úředním věstníku Evropské unie*.

V Bruselu dne 30. července 2020.

Za Radu
předseda
M. ROTH

PŘÍLOHA

Na seznam fyzických a právnických osob, subjektů a orgánů obsažený v příloze rozhodnutí (SZBP) 2019/797 se doplňují tyto osoby a subjekty nebo orgány:

„A. Fyzické osoby

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
1.	GAO Qiang (Kao Čchiang)	Místo narození: provincie Šan-tung, Čína Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin (Tchien-ťin), Čína Státní občanství: čínské Pohlaví: muž	Kao Čchiang je zapojen do „operace Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy. „Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v Unii, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty. „Operaci Cloud Hopper“ provedl aktér veřejně známý jako „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, Stone Panda“, „MenuPass“ a „Potassium“). Kao Čchiang může být s aktérem APT10 spojen, a to i prostřednictvím svého napojení na řídicí a kontrolní infrastrukturu aktéra APT10. Kromě toho byl Kao Čchiang zaměstnán u společnosti Huaying Haitai, což je subjekt označený z důvodu poskytování podpory pro „operaci Cloud Hopper“ a napomáhání k ní. Má vazby na Čang Š'-lunga, který je v souvislosti s „operací Cloud Hopper“ rovněž označen. Kao Čchiang je proto spojen jak se společností Huaying Haitai, tak i s Čang Š'-lungem.	30. 7 .2020
2.	ZHANG Shilong (Čang Š'-lung)	Adresa: Hedong, Yuyang Road No 121, Tianjin (Tchien-ťin), Čína Státní občanství: čínské Pohlaví: muž	Čang Š'-lung je zapojen do „operace Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy. „Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v EU, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty. „Operaci Cloud Hopper“ provedl aktér veřejně známý jako „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“).	30. 7. 2020

			Čang Š'-lung může být s aktérem APT10 spojen, a to i prostřednictvím malwaru, který v souvislosti s kybernetickými útoky provedenými aktérem APT10 vyvinul a otestoval. Kromě toho byl Čang Š'-lung zaměstnán u společnosti Huaying Haitai, což je subjekt označený kvůli poskytování podpory pro „operaci Cloud Hopper" a napomáhání k ní. Má vazby na Kao Čchianga, který je v souvislosti s „operací Cloud Hopper" rovněž označen. Čang Š'-lung je proto spojen jak se společností Huaying Haitai, tak i s Kao Čchiangem.	
3.	Alexey Valeryevich MININ (Alexej Valerjevič Minin)	Алексей Валерьевич МИНИН Datum narození: 27. května 1972 Místo narození: Permská oblast, Ruská SFSR (nyní Ruská federace) Číslo pasu: 120017582 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17. dubna 2017 do 17. dubna 2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní občanství: ruské Pohlaví: muž	Alexej Minin se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku. Jako důstojník pro podporu zpravodajství lidských zdrojů působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Alexej Minin součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na „hacking" do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW.	30. 7. 2020
4.	Aleksei Sergeyvich MORENETS (Alexej Sergejevič Moreněc)	Алексей Сергеевич МОРЕНЕЦ Datum narození: 31. července 1977 Místo narození: Murmanská oblast, Ruská SFSR (nyní Ruská federace) Číslo pasu: 100135556 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17. dubna 2017 do 17. dubna 2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní občanství: ruské Pohlaví: muž	Alexej Moreněc se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku. Jako pracovník pro kybernetické operace působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Alexej Moreněc součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na „hacking" do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW.	30. 7. 2020

5.	Evgenii Mikhaylovich SEREBRIAKOV (Jevgenij Michailovič Serebrjakov)	Евгений Михайлович СЕРЕБРЯКОВ Datum narození: 26. července 1981 Místo narození: Kursk, Ruská SFSR (nyní Ruská federace) Číslo pasu: 100135555, Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost: od 17. dubna 2017 do 17. dubna 2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní občanství: ruské Pohlaví: muž	Jevgenij Serebrjakov se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku. Jako pracovník pro kybernetické operace působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Jevgenij Serebrjakov součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na „hacking“ do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW.	30. 7. 2020
6.	Oleg Mikhaylovich SOTNIKOV (Oleg Michajlovič Sotnikov)	Олег Михайлович СОТНИКОВ Datum narození: 24. srpna 1972 Místo narození: Uljanovsk, Ruská SFSR (nyní Ruská federace) Číslo pasu: 120018866 Vydalo: Ministerstvo zahraničních věcí Ruské federace Platnost. od 17. dubna 2017 do 17. dubna 2022 Místo výkonu zaměstnání: Moskva, Ruská federace Státní občanství: ruské Pohlaví: muž	Oleg Sotnikov se podílel na pokusu o kybernetický útok s potenciálně významným dopadem na Organizaci pro zákaz chemických zbraní (OPCW) v Nizozemsku. Jako důstojník pro podporu zpravodajství lidských zdrojů působící v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU) byl Oleg Sotnikov součástí týmu čtyř ruských vojenských zpravodajských důstojníků, kteří se v dubnu 2018 pokusili získat neoprávněný přístup do bezdrátové sítě organizace OPCW v Haagu (Nizozemsko). Pokus o kybernetický útok byl zaměřen na „hacking“ do bezdrátové sítě organizace OPCW, který by v případě úspěchu ohrozil bezpečnost sítě a probíhající vyšetřovací činnost této organizace. Nizozemská obranná zpravodajská a bezpečnostní služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok zmařila, čímž zabránila vážným škodám pro organizaci OPCW.	30. 7. 2020

B. Právnické osoby, subjekty a orgány

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd	Také známa jako: Haitai Technology Development Co. Ltd Místo: Tchien-ťin, Čína	Společnost Huaying Haitai poskytovala finanční, technickou nebo materiální podporu pro „operaci Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy, a k této operaci napomáhala.	30. 7. 2020

			„Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v Unii, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty. „Operaci Cloud Hopper“ provedl aktér veřejně známý jako „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“). Společnost Huaying Haitiai může být s aktérem APT10 spojena. Kromě toho společnost Huaying Haitai zaměstnávala Kao Čchianga a Čang Š'-lunga, kteří jsou oba v souvislosti s „operací Cloud Hopper“ označeni. Společnost Huaying Haitia je proto s Kao Čchiangem a Čang Š'-lungem spojena.	
2.	Chosun Expo	Také známa jako: Chosen Expo; Korea Export Joint Venture Místo: KLDR	Společnost Chosun Expo poskytla finanční, technickou nebo materiální podporu pro sérii kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy, jakož i s významným dopadem na třetí státy, včetně kybernetických útoků veřejně známých jako „WannaCry“ a kybernetických útoků na polský Úřad pro finanční dozor a společnost Sony Pictures Entertainment, jakož i kybernetické krádeže z banky Bangladesh Bank a pokusu o kybernetickou krádež z banky Vietnam Tien Phong Bank. Kybernetické útoky „WannaCry“ narušily fungování informačních systémů po celém světě tím, že se zaměřily na informační systémy pomocí ransomwaru a zablokovaly přístup k údajům. Měly nepříznivý dopad na informační systémy společností v Unii, včetně informačních systémů týkajících se služeb nezbytných pro udržování základních služeb a hospodářských činností v členských státech. Kybernetické útoky „WannaCry“ provedl aktér veřejně známý jako „APT38“ („Advanced Persistent Threat 38“) a skupina „Lazarus Group“. Společnost Chosun Expo může být na aktéra APT38 nebo skupinu Lazarus Group napojena, a to i prostřednictvím účtů používaných pro kybernetické útoky.	30. 7. 2020
3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) (Hlavní středisko pro speciální technologie (GTsST) hlavního ředitelství generálního štábu ozbrojených sil	Adresa: Ul. Kirova 22, Moskva, Ruská federace	Hlavní středisko pro speciální technologie (GTsST) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GU/GRU), známé rovněž pod svým systémovým identifikačním číslem 74455, je odpovědné za kybernetické útoky s významným dopadem pocházející ze zemí mimo Unii a představující vnější hrozbu pro Unii nebo její členské státy a za kybernetické útoky s významným dopadem na třetí státy, včetně kybernetických útoků veřejně známých jako „NotPetya“ nebo „EternalPetya“ provedených v červnu 2017 a kybernetických útoků namířených na ukrajinskou elektrickou rozvodnou síť v zimě 2015 a 2016.	30. 7. 2020“

	Ruské federace (GU/GRU))		Kybernetické útoky „NotPetya“ nebo „EternalPetya“ znemožnily přístup k údajům v řadě společností v Unii, v širší Evropě a po celém světě tím, že se zaměřily na počítače pomocí ransomwaru a zablokovaly přístup k údajům, což mělo mimo jiné za následek významné ekonomické ztráty. Kybernetický útok na ukrajinskou elektrickou rozvodnou síť způsobil, že její části byly během zimy odpojeny. Za útokem na ukrajinskou elektrickou síť, který byl proveden pomocí útoků „NotPetya“ nebo „EternalPetya“, stál aktér veřejně známý jako „Sandworm“ (také znám jako „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ a „Telebots“). Hlavní středisko pro speciální technologie v rámci hlavního ředitelství generálního štábu ozbrojených sil Ruské federace se aktivně podílí na kybernetických činnostech prováděných aktérem Sandworm a může být na tohoto aktéra napojeno.“	