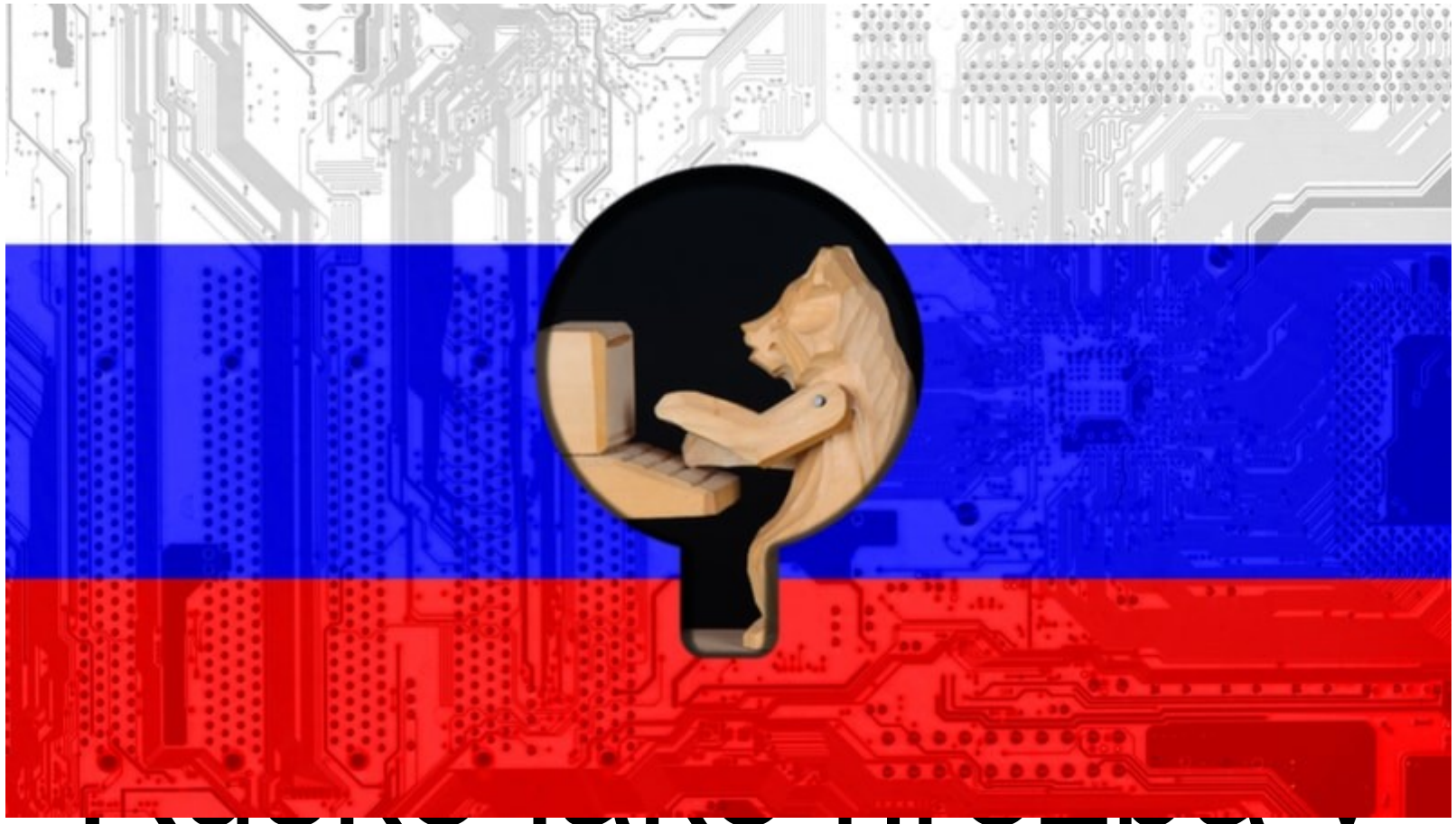


Ruské jako hrozba v kyberprostoru

Michael Myklín, 3.10.2019

National Cyber and Information Security Agency

Michael Myklín

- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)
- Oddělení strategických analýz a informací
- Post-sovětský prostor

- Masarykova univerzita (Bc. a Mgr.)
- Ph.D. in progress (Panslavism in Russian Psychological Operations, Case Study of Czech Republic)

National Cyber and Information Security Agency

Obsah prezentace

- Kyber elementy v ruském strategickém myšlení
  - Ofenzivní kybernetické kapacity
  - Kapacity kybernetické bezpečnosti a „surveillance state“
  - Co Kreml chce, abyste si mysleli vs. skutečnost

- Ruská kyber hrozba vůči České republice
  - Kybernetické útoky proti českému Ministerstvu zahraničních věcí ČR
  - Ruští hackeři v Praze
  - Případ Koněv – útoky, které se nestaly
  - Výzva ruské kyber hrozby pro Českou republiku (a jinde)

National Cyber and Information Security Agency

Kyber v ruském strategickém m

- Znej svého nepřítele, hlavně pokud o něm často píšeš
- Rozdílné chápání kyber prvků
- Informační válka (Informacionnaja vojna)
  - Informačně-psychologické operace – škodlivý obsah (desinformace)
  - Informačně-technické operace – škodlivý kód (malware)
  - Informačně-kinetické operace? - fyzická destrukce nebo kontrola nad „informačním cílem“ internetové kabely, TV/rádio stanice)

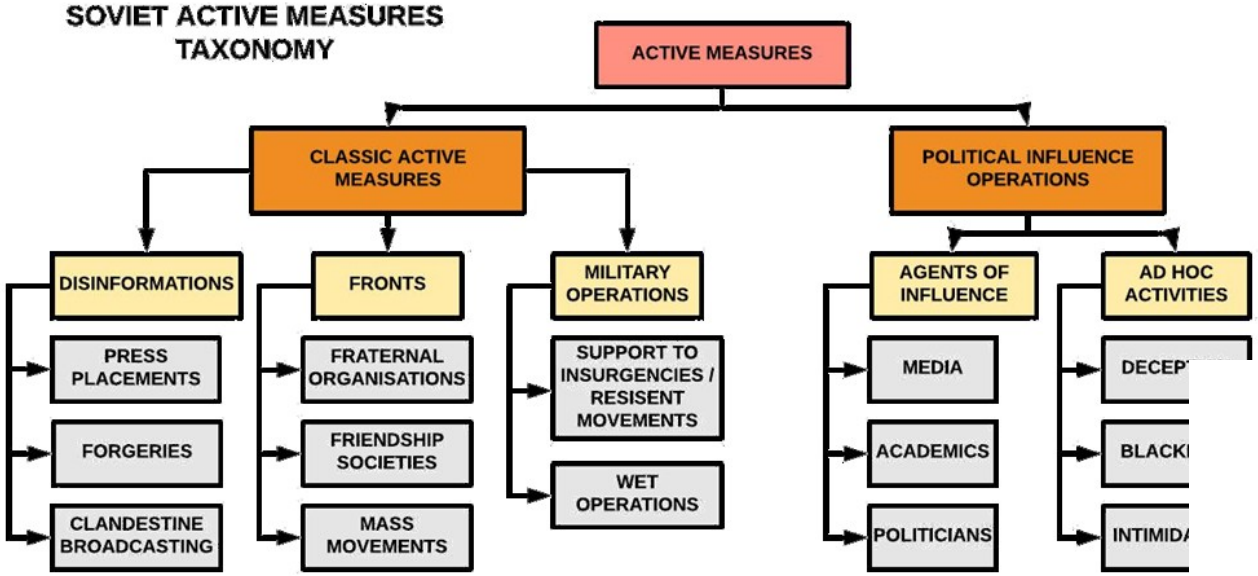
National Cyber and Information Security Agency

Informační válka a kde se vzala

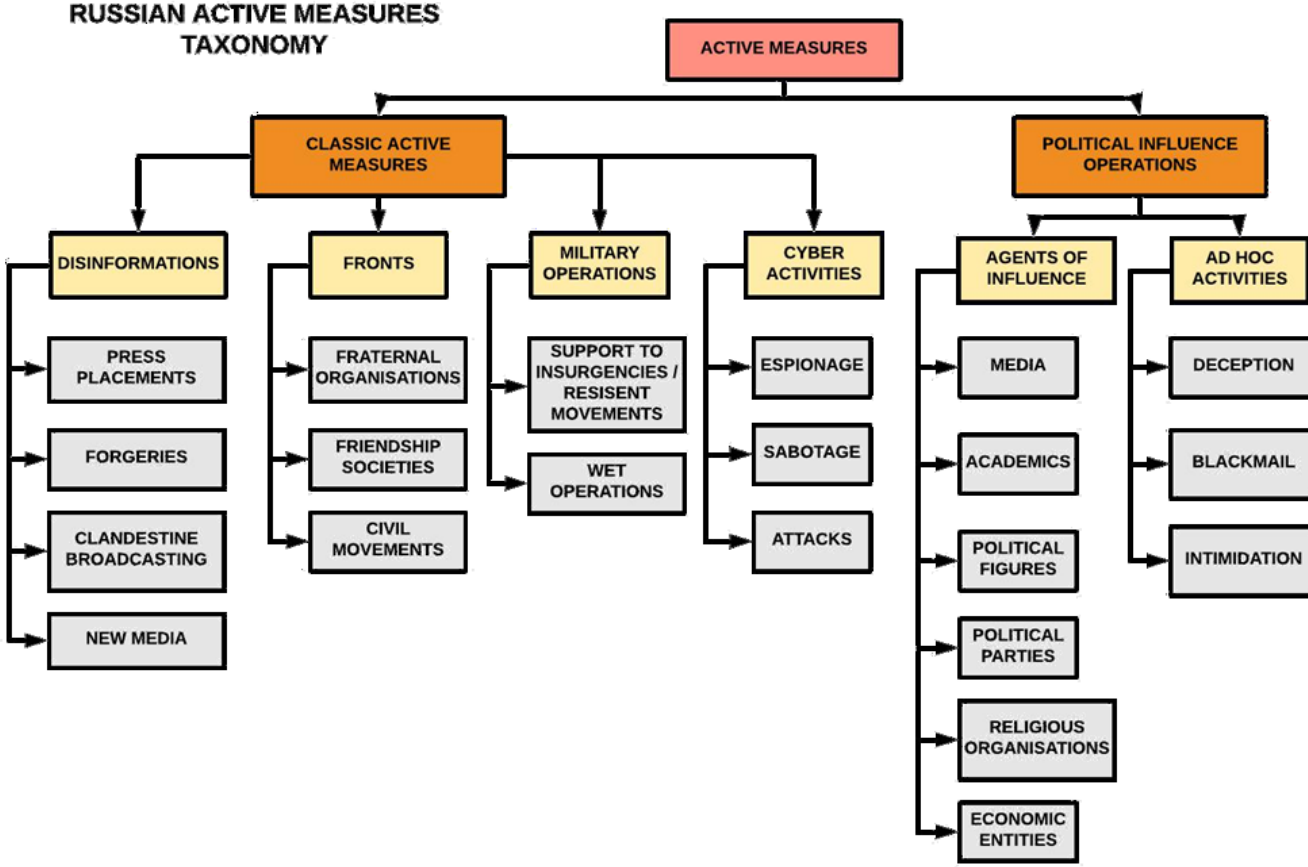
- Sovětský odkaz
  - Aktivní opatření (KGB)
  - Maskirovka (armáda, GRU)
  - Rozvoj technologií
- 1991 – 2019 aka Highway to hell
  - Ztráta ideologie
  - Vladimír Putin a silovici
  - Rostoucí paranoia
  - Internet
  - Nová studená válka

National Cyber and Information Security Agency

SOVIET ACTIVE MEASURES TAXONOMY



RUSSIAN ACTIVE MEASURES TAXONOMY



Kyber v ruském strategickém m

- Znej svého nepřítele, hlavně pokud o něm často píšeš
- Rozdílné chápání kyber prvků
- Informační válka (Informacionnaja vojna)
  - Informačně-psychologické operace – škodlivý obsah (desinformace)
  - Informačně-technické operace – škodlivý kód (malware)
  - Informačně-kinetické operace? - fyzická destrukce nebo kontrola nad „informačním cílem“ internetové kabely, TV/rádio stanice)

- Rusko: Koncept hybridní válka/hybrid warfare/gibridnaja vojna jako výmysl Západu k oslabení Ruska Překvapivá transparence aneb kdo hledá, ten najde
  - Strategické dokumenty
  - Články v akademických časopisech (vojenských)
  - Práce relevantních ruských/sovětských vojenských teoretiků (Kartapolov, Čekinov & Bogdanov, Slipčenko, Messner)

National Cyber and Information Security Agency

Kyber v ruském strategickém my

- Znej svého nepřítele, hlavně pokud o něm často píšeš
- Rozdílné chápání kyber prvků
- Informační válka (Informacionnaja vojna)
  - Informačně-psychologické operace – škodlivý obsah (desinformace)
  - Informačně-technické operace – škodlivý kód (malware)
  - Informačně-kinetické operace? - fyzická destrukce nebo kontrola nad „informačním cílem“ internetové kabely, TV/rádio stanice)
- Koncept hybridní válka/hybrid warfare/gibridnaja vojna = Západní výmysl k oslabení Ruska (ruský postoj)
- Překvapivá transparence aneb kdo hledá, ten najde
  - Strategické dokumenty
  - Články v akademických časopisech (vojenských)
  - Práce relevantních ruských/sovětských vojenských teoretiků (Kartapolov, Čekinov & Bogdanov, Slipčenko, Messner)

Ofenzivní kybernetické kapacity

- Většina ofenzivních kybernetických kapacit v rukou zpravodajských služeb
- FSB, GRU and SVR
  - Více státní kontroly, méně útoků patriotických hackerů (na Západě)

- Lepší, silnější a rychlejší malware i útočníci
  - Crowdstrike: Ruské APT skupiny jako nejlepší na světě?

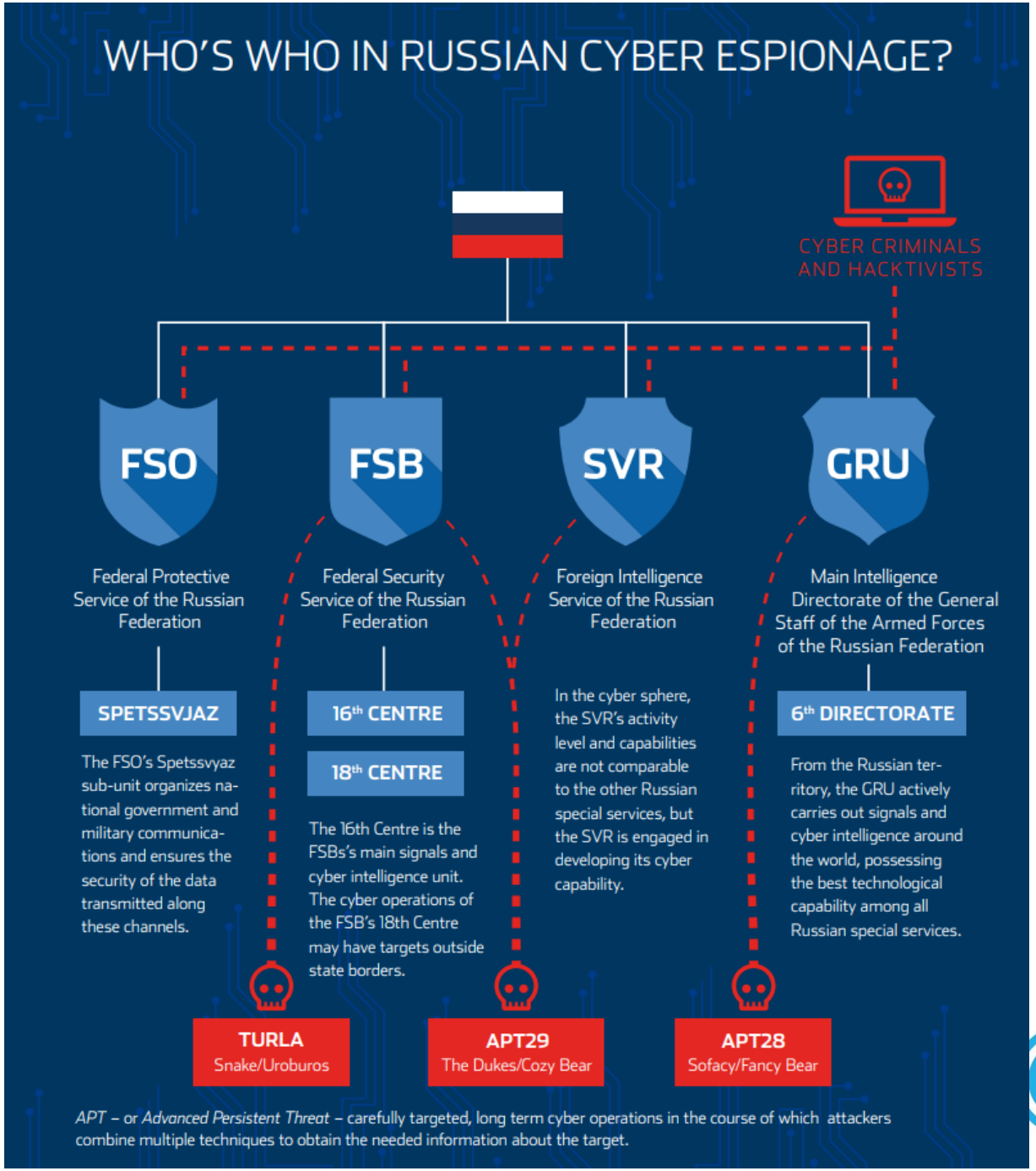
- Více jak tucet APT skupin s různou úrovní zkušeností, schopností nástrojů a cílů
  - Nejhorší na skupinách útočníků nejsou útoky, ale názvy skupin

- Špionáž
  - Ekonomická (letecký, vesmírný, farmaceutický, zbrojní průmysl)
  - Vlády (DNC, Bundestag, MFA´s)
  - Průmysl (kritická infrastruktura)
- Sabotáž
  - Ransomware/wiper (Maersk)
  - Průmyslová sabotáž (ukrajinská rozvodná síť, saudský petro-chemický závod)

National Cyber and Information Security Agency

APT = Advanced Persistent Threat / pokročilá trvalá hrozba

- Sofistikované skupiny hackerů, které jsou schopny se do systémů oběti dostat nepozorovaně a nepozorovaně v nich po delší dobu působit
- Často navázané na státní aktéry



Ofenzivní kybernetické kapacity

- Většina ofenzivních kybernetických kapacit v rukou zpravodajských služeb
- FSB, GRU and SVR
  - Více státní kontroly, méně útoků patriotických hackerů (na Západě)

- Lepší, silnější a rychlejší malware i útočníci
  - Crowdstrike: Ruské APT skupiny jako nejlepší na světě?

- Více jak tucet APT skupin s různou úrovní zkušeností, schopností nástrojů a cílů
  - Nejhorší na skupinách útočníků nejsou útoky, ale názvy skupin

- Špionáž
  - Ekonomická (letecký, vesmírný, farmaceutický, zbrojní průmysl)
  - Vlády (DNC, Bundestag, MFA´s)
  - Průmysl (kritická infrastruktura)
- Sabotáž
  - Ransomware/wiper (Maersk)
  - Průmyslová sabotáž (ukrajinská rozvodná síť, saudský petro-chemický závod)

National Cyber and Information Security Agency

Dostupné: https://crowdstrike.lookbookhq.com/web-global-threat-report-2019/crowdstrike-2019-gtr?utm_campaign=Threat_Report_2019

National Cyber and Information Security Agency

Ofenzivní kybernetické kapacity

- Většina ofenzivních kybernetických kapacit v rukou zpravodajských služeb
- FSB, GRU and SVR
  - Více státní kontroly, méně útoků patriotických hackerů (na Západě)

- Lepší, silnější a rychlejší malware i útočníci
  - Crowdstrike: Ruské APT skupiny jako nejlepší na světě?

- Více jak tucet APT skupin s různou úrovní zkušeností, schopností nástrojů a cílů
  - Nejhorší na skupinách útočníků nejsou útoky, ale názvy skupin

- Špionáž
  - Ekonomická (letecký, vesmírný, farmaceutický, zbrojní průmysl)
  - Vlády (DNC, Bundestag, MFA´s)
  - Průmysl (kritická infrastruktura)
- Sabotáž
  - Ransomware/wiper (Maersk)
  - Průmyslová sabotáž (ukrajinská rozvodná síť, saudský petro-chemický závod)

National Cyber and Information Security Agency

Ofenzivní kybernetické kapacity

- Většina ofenzivních kybernetických kapacit v rukou zpravodajských služeb
- FSB, GRU and SVR
  - Více státní kontroly, méně útoků patriotických hackerů (na Západě)

- Lepší, silnější a rychlejší malware i útočníci
  - Crowdstrike: Ruské APT skupiny jako nejlepší na světě?

- Více jak tucet APT skupin s různou úrovní zkušeností, schopností nástrojů a cílů
  - Nejhorší na skupinách útočníků nejsou útoky, ale názvy skupin

Name #1	Name #2	Name #3	Name #4	Name #5	Name #6	Name #7
APT 28	Sofacy	Fancy Bear	Pawn Storm	Strontium	Tsar Team	Sednit
APT 29	Dukes	Cozy Bear	Cozy Duke	EuroAPT	CozyCar	Group 100
Turla	Snake	Uroboros	Venomous Bear	Krypton	Waterbug	Group 88

Ofenzivní kybernetické kapacity

- Většina ofenzivních kybernetických kapacit v rukou zpravodajských služeb
- FSB, GRU and SVR
  - Více státní kontroly, méně útoků patriotických hackerů (na Západě)

- Lepší, silnější a rychlejší malware i útočníci
  - Crowdstrike: Ruské APT skupiny jako nejlepší na světě?

- Více jak tucet APT skupin s různou úrovní zkušeností, schopností nástrojů a cílů
  - Nejhorší na skupinách útočníků nejsou útoky, ale názvy skupin

- Špionáž
  - Ekonomická (letecký, vesmírný, farmaceutický, zbrojní průmysl)
  - Vlády (DNC, Bundestag, MFA´s)
  - Průmysl (kritická infrastruktura)
- Sabotáž
  - Ransomware/wiper (Maersk)
  - Průmyslová sabotáž (ukrajinská rozvodná síť, saudský petro-chemický závod)

National Cyber and Information Security Agency

Kapacity kybernetické bezpečnosti a „surveillance state“

- Masivní aparát vytvořený ke kontrole ruského internetu, jeho uživatelů a k ochraně ruské telekomunikační infrastruktury
- Řada zákonů dávají státu nemalý vliv
  - Federální zákon č. 40-FZ - Zákon o Federální bezpečnostní službě
  - Federální zákon č. 241-FZ - Zákaz anonymních komunikačních aplikací (Instant Messaging, IM)
  - Federální zákon č. 242-FZ - Povinnost sběru, ukládání a zpracování osobních údajů ruských občanů na serverech v Rusku
  - Federální zákon č. 28-FZ - Šíření fake news je trestáno pokutou. Týká se pouze online médií
- Alespoň 44 institucí a organizací zabývajících se kybernetickou bezpečnostní/informační válkou
- Izolovaný RuNet jako dlouhodobý plán?

National Cyber and Information Security Agency

Federální zákon č. 40-FZ - Zákon o Federální bezpečnostní službě

- *„Státní orgány, stejně jako firmy, vědecké instituce a další organizace **jsou povinny poskytovat orgánům FSB podporu** v plnění jim uložených úkolů.*

- *Fyzické i právnické osoby v Ruské Federaci zajišťující poštovní služby, **telekomunikační spojení všeho druhu**, včetně systémů elektronické, důvěrné a satelitní komunikace, jsou povinny na žádost FSB instalovat do svých systémů doplňková zařízení a software, a zajistit vhodné podmínky nutné pro operativní a technická opatření FSB.*

- *V rámci plnění úkolů pro zajištění bezpečnosti Ruské federace **mohou být příslušníci FSB přiřazeni ke státním orgánům, firmám, výzkumným institucím nebo jiným organizacím nezávisle na jejich formě vlastnictví**, a to se souhlasem vedoucích pracovníků, přičemž zůstávají ve vojenské službě.“*

National Cyber and Information Security Agency

Kapacity kybernetické bezpečnosti a „surveillance state“

- Masivní aparát vytvořený ke kontrole ruského internetu, jeho uživatelů a k ochraně ruské telekomunikační infrastruktury
- Řada zákonů dávají státu nemalý vliv
  - Federální zákon č. 40-FZ - Zákon o Federální bezpečnostní službě
  - Federální zákon č. 241-FZ - Zákaz anonymních komunikačních aplikací (Instant Messaging, IM)
  - Federální zákon č. 242-FZ - Povinnost sběru, ukládání a zpracování osobních údajů ruských občanů na serverech v Rusku
  - Federální zákon č. 28-FZ - Šíření fake news je trestáno pokutou. Týká se pouze online médií
- Alespoň 44 institucí a organizací zabývajících se kybernetickou bezpečnostní/informační válkou
- Izolovaný RuNet jako dlouhodobý plán?

National Cyber and Information Security Agency

Co Kreml chce, abyste si mysleli vs. skutečnost

- Rusko - schopné, nebezpečné, ale stále jen státní aktér se všemi plusy i mínusy, které s tím souvisí

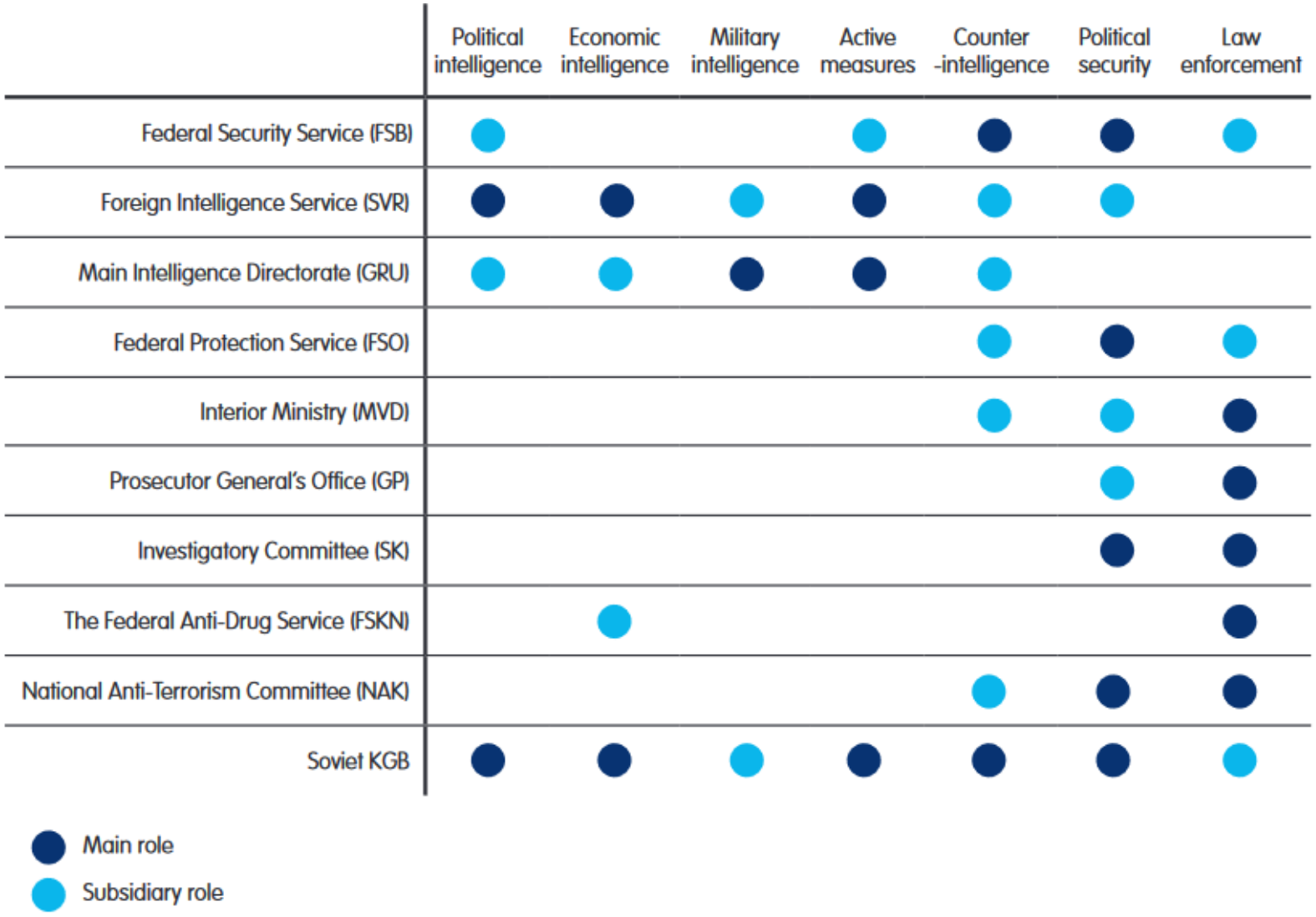
JAKÉ???

National Cyber and Information Security Agency

Co Kreml chce, abyste si mysleli vs. skutečnost

- Rusko - schopné, nebezpečné, ale stále jen státní aktér se všemi plusy i mínusy, které s tím souvisí
- Korupce, byrokracie, lenost, překrývající se jurisdikce, politické hašteření a chyby
- Ruské kapacity i schopnosti jsou občas přeháněny
- TLDR: Not great, not terrible

National Cyber and Information Security Agency



Zdroj: Galeotti, Mark. 2016. Putin's hydra: Inside Russia's intelligence services. ECFR

National Cyber and Information Security Agency

Co Kreml chce, abyste si mysleli vs. skutečnost

- Rusko - schopné, nebezpečné, ale stále jen státní aktér se všemi plusy i mínusy, které s tím souvisí
- Korupce, byrokracie, lenost, překrývající se jurisdikce, politické hašteření a chyby
- Ruské kapacity i schopnosti jsou občas přeháněny
- TLDR: Not great, not terrible

National Cyber and Information Security Agency

Russia's Secret Intelligence Agency Hacked: 'Largest Data Breach In Its History'

Zak Doffman Contributor ⓘ
Cybersecurity
I write about security and surveillance.

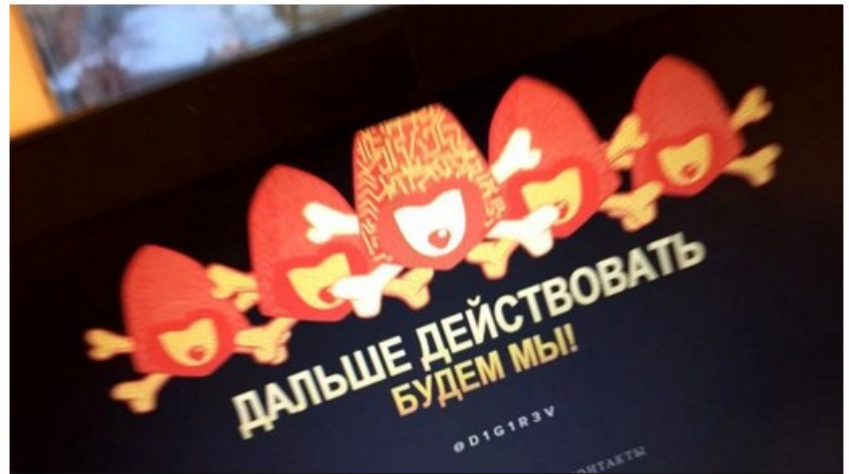
GETTY

Red faces in Moscow this weekend, with the news that hackers have successfully targeted FSB—Russia's Federal Security Service. The hackers managed to steal 7.5 terabytes of data from a major contractor, exposing secret FSB projects to de-anonymize Tor browsing, scrape social media, and help the state split its internet off from the rest of the world. The data was passed to mainstream media outlets for publishing.

"Стоп-слово" - Навальный. Хакеры разоблачили "проект ФСБ" в соцсетях

Андрей Сошников, Андрей Захаров
Би-би-си

20 декабря 2018 Поделиться



Digital Revolution часто цитируют Виктора Цоя, а свой первый твит "настало время освободить Рунет" они сопроводили треком рэпера Влади

Хакеры из группы Digital Revolution утверждают, что взломали сервер НИИ "Квант", принадлежащего ФСБ. Опубликованные ими документы описывают систему мониторинга соцсетей, основная цель которой - анализ протестных настроений. Такую систему "Квант" в качестве субподрядчика уже реализует в Казахстане, узнала Би-би-си.

ПОЛИТИКА

Штирлиц близок к провалу. Мэрия Москвы выложила в открытый доступ адреса более чем тысячи сотрудников СВР

· *Сергей Канев · 04.06.2019 11:50*

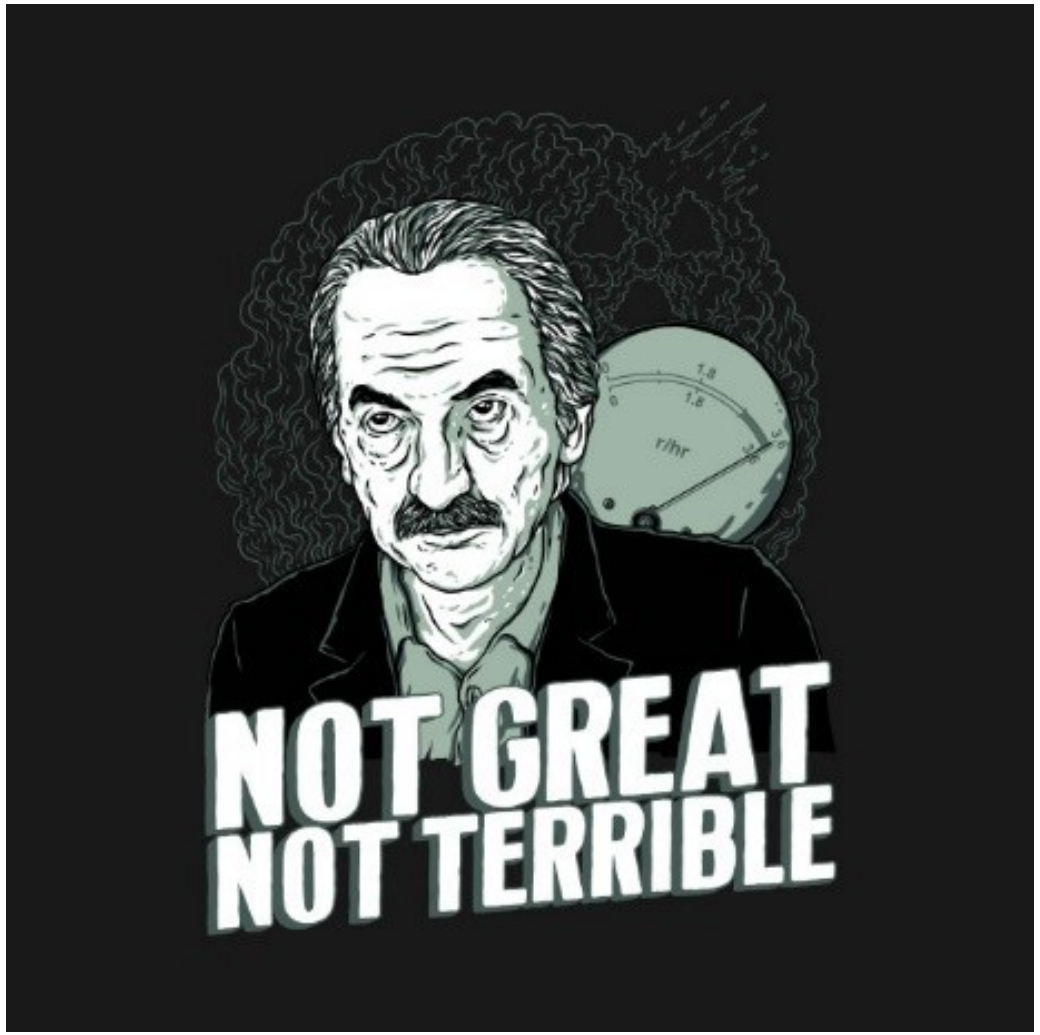
Читатели The Insider знают, насколько небрежно российские спецслужбы относятся к своей конспирации. Так, например, в открыто продающейся базе должников по кредитам обнаруживаются сотрудники засекреченных подразделений ФСБ, а в базе ГИБДД можно найти все персональные данные сотен сотрудников ГРУ. Как выяснил The Insider, СВР оказалась еще более прозрачной организацией: в открытом доступе на официальном сайте мэрии Москвы можно обнаружить адреса ведомственных домов Службы внешней разведки, где получили квартиры несколько тысяч офицеров. Чтобы получить их данные, не нужны даже никакие доступы к базам, любой желающий может

National Cyber and Information Security Agency

Co Kreml chce, abyste si mysleli vs. skutečnost

- Rusko - schopné, nebezpečné, ale stále jen státní aktér se všemi plusy i mínusy, které s tím souvisí
- Korupce, byrokracie, lenost, překrývající se jurisdikce, politické hašteření a chyby
- Ruské kapacity i schopnosti jsou občas přeháněny
- TLDR: Not great, not terrible

National Cyber and Information Security Agency



National Cyber
and Information
Security Agency

Ruská kyber hrozba vůči České republice

Případy a poučení:

- Ministerstvo zahraničních věcí ČR
- Ruští hackeři v Praze
- Případ Koněv – útoky, které se nestaly
- Výzva ruské kyber hrozby pro Českou republiku (a jinde)

National Cyber and Information Security Agency

Kybernetické útoky proti Ministerstvu zahraničí

- Několik rozsáhlých špionážních kampaní proti MZV
  - Podezřelí jsou ruští a čínští hackeři
- 2016/17
  - Více než 150 e-mailových účtů kompromitováno, včetně těch patřících nejvyššímu vedení (Turla/FSB)
  - Brute-force útoky proti e-mailovým účtům (Sofacy/GRU)
- 2019
  - Česká stálá delegace při NATO HQ
  - Deník N: Ruští hackeři zodpovědní za útok

National Cyber and Information Security Agency

Ruští hackeři v Praze

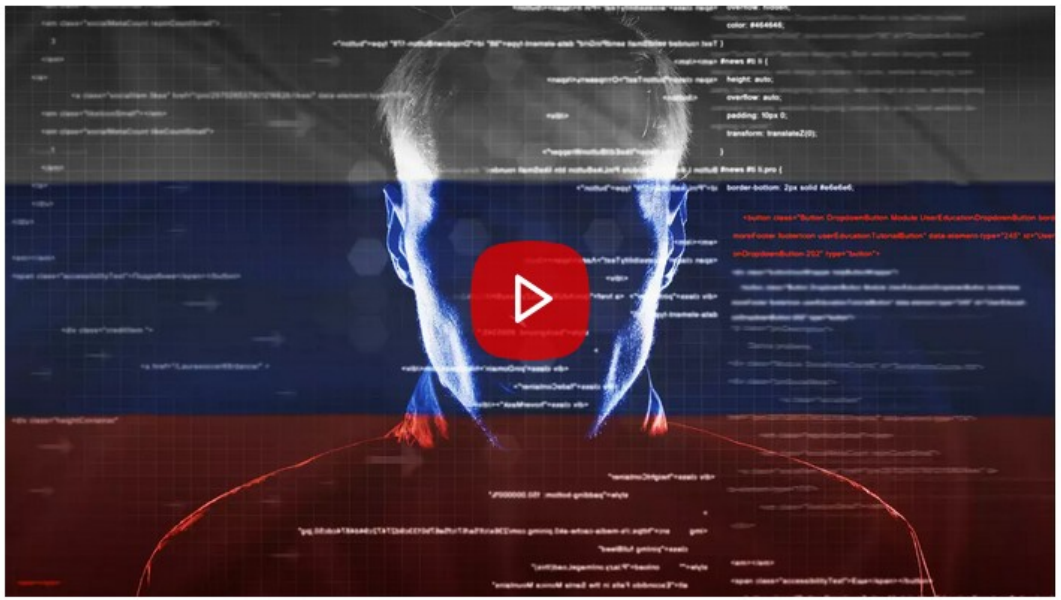
- FSB využívalo dvě české IT společnosti jako krytí pro hackery a jejich aktivity
- Operace odkryta Bezpečnostní informační službou (BIS)

- Poučení?
  - Ruští hackeři operují i mimo území Ruska, dokonce ve státech NATO a delší časové období. Proč v Praze?
    - Podpora z ambasády
    - Zakrýt původce útoku
    - Blízkost k cíli (HUMINT)

National Cyber and Information Security Agency

Ruští špioni v Česku operovali pod krytím IT firem. Někteří měli české občanství

Lucie Hrdličková , Martin Zíta 19. 3. 2019



Reportér Respektu Ondřej Kundra o ruských špionech na českém území. (Video: Seznam.cz)

Pod krytím dvou pražských firem údajně v Česku fungovala ruská špionská skupina, ve které figurovali Rusové s českým občanstvím. Skupina měla stát například za hackerskými útoky. Informoval o tom týdeník Respekt.

Firmy podle dostupných informací na veřejnosti vystupovaly jako prodejci počítačového hardwaru a softwaru. České úřady je měly sledovat několik let. Systém na hackování měl být umístěn ve firemních počítačích.

Případ Koněv – útoky, které se nestaly

- Ruské MZV nespokojené s plány na přesun/odstranění sochy Maršála Ivana Koněva z jeho původního místa
- Podobnost případu s Estonskem (2007)
  - Přesun bronzové sochy sovětského vojáka
  - Kyber útoky (DDoS) proti estonským státních institucím, bankám a médiím

- NÚKIB počítal s možností útoků, ale nic se nestalo

- Reflexiní operace české kontrarozvědky nebo jen šťastná náhoda?
  - Identifikace proruských skupin

National Cyber and Information Security Agency

National Cyber
and Information
Security Agency

Koněv case – attacks that didn´t happen

- Ruské MZV nespokojené s plány na přesun/odstranění sochy Maršála Ivana Koněva z jeho původního místa
- Podobnost případu s Estonskem (2007)
  - Přesun bronzové sochy sovětského vojáka
  - Kyber útoky (DDoS) proti estonským státních institucím, bankám a médiím

- NÚKIB počítal s možností útoků, ale nic se nestalo

- Reflexiní operace české kontrarozvědky nebo jen šťastná náhoda?
  - Identifikace proruských skupin

National Cyber and Information Security Agency

Koněv case – attacks that didn´t happen

- Ruské MZV
  Ivana Koněv
- Podobnost p
  - Přesun bro
  - Kyber útok

- NÚKIB počít

- Reflexiní ope
  - Identifikac

y Maršála

a médiím

hoda?

National Cyber
and Information
Security Agency

Koněv case – attacks that didn´t happen

- Ruské MZV nes … sochy Maršála Ivana Koněva z
- Podobnost příp
  - Přesun bronz
  - Kyber útoky (… kám a médiím
- NÚKIB počítal s
- Reflexiní opera … ná náhoda?
  - Identifikace p

[redacted]

Procházet zastupitelským emailem není před hlasováním o Koněvovi žádný med. Ale aspoň si osvěžím znalosti zvláštních spolků. Píší, řazeno abecedně:

1. Asociace absolventů ruských (sovětských) vysokých škol, z. s., Vladimír Pick, předseda
2. Aliance národních sil, Vladimíra Vítová, předsedkyně
3. Asociace nezávislých médií, z.s., Stanislav Novotný, předseda
4. České mírové hnutí, z. s., Milan Krajča, předseda
5. Česká společnost pro civilizační studia, z.s., Petr Hampl, tajemník
6. Česko-ruská společnost, z. s., Jiří Klapka, předseda
7. Československí vojáci v záloze za mír, z. s., Ivan Kratochvíl, velitel
8. Hej, občané!, z. s., Žarko Jovanovič
9. Magistra Vitae, z. s., Josef Skála, předseda
10. Národní domobrana, z. s., Marek Obrtel, předseda
11. NE základnám ČR, z. s., Václav Novotný, předseda
12. Slovanský výbor, z. s., Jan Minář, předseda
13. Společnost Julia Fučíka, z. s., Jan Jelínek, předseda
14. Spolek českých novinářů, z.s., Pavel Novák, předseda
15. Unie českých spisovatelů, Karel Sýs, předseda
16. Vlastenecké sdružení antifašistů ČR, z. s., Josef Liška, místopředseda
17. Vojáci proti válce, z. s., Jiří Bureš, předseda

Tento zvláštní spolek se podle jiných kritérií než abecedy radši ani řadit neodvážím, některé podle jména znám, některé jsem měl za léta zaniklé (NE základnám stále žije?) a taková asociace absolventů ruských škol mne vyslovene překvapila.

National Cyber and Information Security Agency

Výzva ruské kyber hrozby pro Českou republiku (a jinde)

- Nedostatek peněz na lidi, vzdělávání a nástroje (HW, SW) ve státních institucí
- Rozpačité reakce vlády na kybernetické útoky
- Nejasné vztahy mezi státem a soukromými společnostmi v Rusku
  - Nejde o takový extrém jako v Číně, ale ruský legislativní rámec zaslouží pozornost
  - Je bezpečné spolupracovat s ruskými společnostmi?

National Cyber and Information Security Agency

Available on: https://www.nukib.cz/cs/informacni-servis/publikace/

National Cyber and Information Security Agency

Děkuji za pozornost

Otázky?

m.myklin@nukib.cz

National Cyber and Information Security Agency