TECHNOLOGICKÉ CENTRUM PRAHA

PROSINEC 2024

STUDIE TRHU BEZPEČNOSTNÍCH A OBRANNÝCH TECHNOLOGIÍ V ČR

AUTOŘI:

VLADISLAV ČADIL, ADÉL KUČERA – TECHNOLOGICKÉ CENTRUM PRAHA

Studie trhu bezpečnostních a obranných technologií v ČR

Prosinec 2024

Autoři

Vladislav Čadil, Adél Kučera – Technologické centrum Praha

Tato studie je výsledkem projektu Systém pro strategické řízení bezpečnostního výzkumu (VK01020207), podpořeného Ministerstvem vnitra ČR v programu VK – Otevřené výzvy v bezpečnostním výzkumu 2023-2029 (OPSEC).

Obsah

Shrnutí

Tato studie je jedním z výsledků projektu Systém pro strategické řízení bezpečnostního výzkumu (VK01020207), podpořeného Ministerstvem vnitra ČR. Cílem Studie trhu bezpečnostních a obranných technologií v ČR bylo charakterizovat trh bezpečnostních technologií v ČR, zejména identifikovat nabídku technologií a řešení v jednotlivých oblastech bezpečnosti – kybernetické bezpečnosti, krizovém řízení, vymáhání práva a CBRN hrozbách – a dále identifikovat specifické tematické skupiny v těchto oblastech a jejich rozsah. Účelem této studie bylo (i.) vyzkoušet přístupy a informační zdroje k průzkumu trhu bezpečnostních technologií a (ii.) poskytnout přehled o trhu bezpečnostních a obranných technologiích, který bude možné dále rozšiřovat a prohlubovat. Studie tedy nepřináší detailní analýzu trhu bezpečnostních technologií. Předloženou studii je z tohoto hlediska žádoucí považovat za pilotní, na níž by měly navazovat další, specificky zaměření studie mapující a analyzující trh bezpečnostních a obranných technologií v ČR.

Z důvodu dostupnosti dat analýza trhu kladla větší pozornost na stranu nabídky. Základ použitého metodického přístupu pro analýzu strany nabídky představovala kvalitativní analýza dat o firmách získaných z veřejně dostupných informačních zdrojů – seznamu českých podniků v EU Civil Security Stakeholder catalogue, Informačního systému výzkumu, vývoje a inovací, seznamu členů Asociace obranného a bezpečnostního průmyslu České republiky, katalogů Czech Digital Solutions SystemOnLine a veletrhů IDET 2023 a PYROS – ISET 2023. Firmy byly na základě zaměření svých produktů a aktivit rozčleněny do výše uvedených základních oblastí bezpečnosti. Následně byla provedena kvalitativní segmentační analýza, která v jednotlivých podoblastech identifikovala specifické skupiny produktů (výrobků a služeb) poskytovaných analyzovanými firmami. Identifikované skupiny byly blíže charakterizovány podle popisu produktů a aktivit podniků sdružených v daných skupinách.

Z důvodu nedostupnosti úplných dat o hospodaření podniků a zejména absence informací o mezipodnikových zakázkách byla strana poptávky sledována jen na úrovni poptávky veřejného sektoru, která byla zjišťována podle objemu veřejných zakázek uvedených v Registru smluv. Analýzy poptávky veřejného sektoru však může být omezena tím, že v Registru smluv nejsou uvedeny zakázky s utajovaným obsahem.

Význam jednotlivých oblastí a jejich dílčích segmentů (tematických skupin) na trhu byl následně stanoven podle počtu podniků (ukazatel pro stranu nabídky) a objemu veřejných zakázek v oblasti bezpečnostních technologií (indikátor poptávky veřejného sektoru po bezpečnostních technologiích).

Celkem bylo identifikováno 432 firem podnikajících v oblasti bezpečnostních a obranných technologií. Polovinu z identifikovaných podniků tvoří malé podniky (do 50 zaměstnanců). Takřka dvě třetiny objemu veřejných zakázek však získaly velké firmy (nad 250 zaměstnanců).

Škála produktů a aktivit poloviny sledovaných firem významně přesahuje vymezení jednotlivých oblastí bezpečnostního trhu. Pětina podniků působí současně v oblasti vymáhání práva a krizového řízení a více než desetina podniků v kombinaci oblastí kybernetické bezpečnosti, vymáhání práva a krizového řízení. Z podniků, které působily v jediné oblasti, jich je nejvíce v oblasti kybernetické bezpečnosti (17 % z celkového počtu všech podniků).

V oblasti kybernetické bezpečnosti dvě pětiny podniků působily v tematické skupině *Prevence kyberkriminality a řešení kybernetické bezpečnosti a* téměř čtvrtina se věnovala skupině *Digitální transformace a IT poradenství*. V oblasti krizového řízení přibližně dvě pětiny podniků rozvíjely své aktivity ve skupině *Nouzové a záchranné vybavení* a téměř třetina ve skupině *Komunikační a koordinační (IT) systémy.* V oblasti vymáhání práva nejvíce subjektů působilo ve skupinách *IT řešení pro boj proti kyberkriminalitě* a *Technologie pro krizové řízení využitelné pro vymáhání práva* (po 18,26 %). V oblasti CBRN hrozeb téměř třetina firem podnikala ve skupině *Stavební materiály a konstrukční prvky* a po pětině podniků ve skupinách *Dekontaminace a ochranné prostředky* a *Výzkum a vývoj v oblasti CBRN*.

Dále byla identifikována oblast ostatních firem, do které byly zařazeny podniky, které se specializují spíše na oblast obrany a obranné technologie než na oblast bezpečnosti. Do této oblasti bylo zařazeno 37 podniků. Na základě svého zaměření byly podniky z oblasti „ostatní“ rozděleny do tří specifických skupin: (i.) *Letecká technika*, (ii.) *Obrněná vozidla* a (iii.) *Střelné zbraně*. Dvě pětiny podniků z této oblasti podnikaly ve skupině *Střelné zbraně*.

Sledované podniky v letech 2020-2024 získaly téměř 10 mld. Kč z veřejných zakázek, které směřovaly do oblasti bezpečnostních a obranných technologií. Objem veřejných zakázek je velmi nerovnoměrně distribuován. Polovinu objemu veřejných zakázek získalo pouze 5 podniků, zatímco více než polovina nezískala žádnou veřejnou zakázku v oblasti bezpečnostních technologií.

Nejvyšší poptávka veřejného sektoru po bezpečnostních technologiích nastala v oblastech kybernetické bezpečnosti a krizového řízení. Podniky působící jen v oblasti kybernetické bezpečnosti získaly 38,8 % z celkového objemu zakázek v oblasti bezpečnostních technologií, v oblasti krizového řízení 18,6 % a v kombinaci kybernetické bezpečnosti, vymáhání práva a krizového řízení 15,7 %.

V oblasti kybernetické bezpečnosti získaly dvě pětiny objemu veřejných zakázek podniky z tematické skupiny *Digitální transformace a IT poradenství*. Po zhruba pětině objemu veřejných zakázek obdržely firmy podnikající ve skupinách *Kybernetická bezpečnost kritické infrastruktury* a *Digitální forenzní analýza*. V oblasti krizového řízení nejsilnější poptávka veřejného sektoru nastala ve skupinách *Komunikační a koordinační (IT) systémy* (58,94 % objemu veřejných zakázek) a *Dohledové a bezpečnostní systémy* (32,29 %). V oblasti vymáhání práva nejvyšší objem zakázek byl alokován ve skupinách *Bezpečnostní systémy pro vymáhání práva (*37,21 %) a do skupiny *IT řešení pro boj proti kyberkriminalitě* (30,26 %). V oblasti CBRN hrozeb nejvyšší objem veřejných zakázek obdržely podniky zařazené do skupiny *Výzkum a vývoj v oblasti CBRN* (87,82 %). V oblasti ostatních firem čtyři pětiny objemu veřejných zakázek směřovaly do skupiny *Obrněná vozidla*.

1 Úvod

Cílem Studie trhu bezpečnostních a obranných technologií v ČR bylo charakterizovat trh bezpečnostních technologií v ČR, zejména identifikovat nabídku technologií a řešení v jednotlivých oblastech bezpečnosti – kybernetické bezpečnosti, krizovém řízení, vymáhání práva a CBRN hrozbách – a dále identifikovat specifické tematické skupiny v těchto oblastech a jejich rozsah. Účelem této studie bylo (i.) vyzkoušet přístupy a informační zdroje k průzkumu trhu bezpečnostních technologií a (ii.) poskytnout přehled o trhu bezpečnostních a obranných technologiích, který bude možné dále rozšiřovat a prohlubovat.

Cílem této studie nebylo přinést nějaké hodnocení kvality (resp. novosti) konkrétních technologií nebo řešení a příslušných vývojových trendů včetně predikce vývoje trhu, hodnocení využívání těchto technologií, faktorů, které ovlivňují fungování trhu či formulaci doporučení pro stimulaci a koordinaci rozvoje trhu bezpečnostních technologií. Studie tedy nepřináší detailní analýzu trhu bezpečnostních technologií. Předloženou studii je z tohoto hlediska žádoucí považovat za pilotní, na níž by měly navazovat další, specificky zaměření studie mapující a analyzující trh bezpečnostních a obranných technologií v ČR.

Studie sestává z několika částí. Nejprve je popsána metodika zpracování této studie a informační zdroje, z nichž vychází. Další část přináší základní charakteristiku podniků, které působí v oblasti bezpečnostních technologií. Uvádí jejich velikostní strukturu, objem veřejných zakázek v oblasti bezpečnosti a zastoupení podniků v jednotlivých oblastech bezpečnosti, resp. v jejich kombinacích. Ukazuje, které oblasti a kombinace oblastí představují hlavní část trhu bezpečnostních technologií. Následující část je věnována jednotlivým oblastem bezpečnosti. Je strukturována podle oblastí bezpečnosti. U každé oblasti ukazuje velikostní strukturu podniků a objem veřejných zakázek podle této struktury. Dále přináší rozdělení oblastí do specifických segmentů – tematických skupin. Nejprve stanovuje zastoupení těchto skupin na základě počtu podniků a objemu veřejných zakázek, následně jsou jednotlivé skupiny blíže popsány. Pro nejvíce zastoupené skupiny jsou uvedeny příklady stěžejních podniků, které působí v dané tematické skupině. Závěrečná část shrnuje hlavní zjištění.

2 Metodika

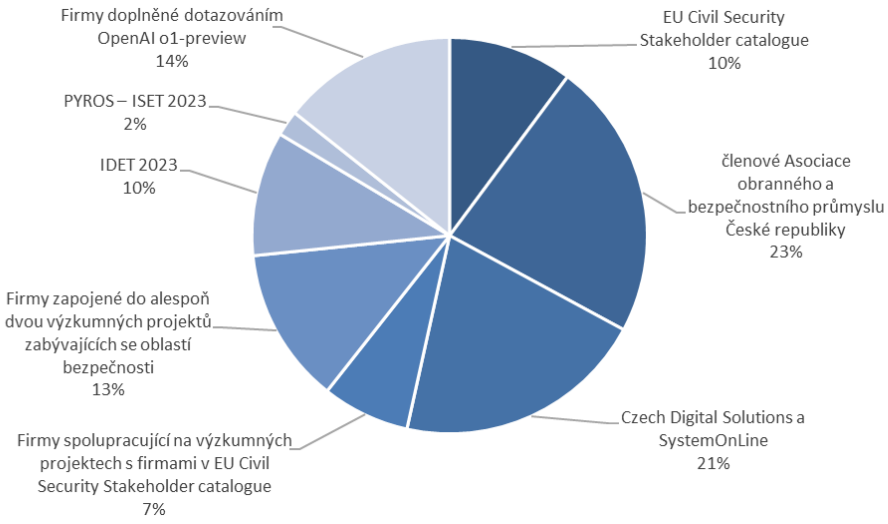
Základ využitého metodického přístupu představuje kvalitativní analýza dat o firmách získaných z veřejně dostupných informačních zdrojů. Nejprve byla pozornost věnována straně nabídky v oblasti bezpečnostních a obranných technologií. Ta byla zjišťována na základě seznamu firem, které podnikají v oblasti bezpečnosti. Tento seznam byl vytvářen se zaměřením na čtyři dílčí podoblasti: kybernetická bezpečnost, vymáhání práva (obzvláště v souvislosti s organizovaným zločinem a terorismem), CBRN hrozby (chemické, biologické, radiologické a nukleární) a krizové řízení (zejména včasná výstraha, krizová komunikace, integrovaný záchranný systém). Při sestavování seznamu bylo cílem zachytit dostatečně široké spektrum firem a nevynechat žádné důležité společnosti. Zdroje pro vytipování firem do seznamu byly poměrně různorodé, takže se můžeme domnívat, že většina společností podnikajících ve vymezené oblasti byla do seznamu zahrnuta.

U všech vytipovaných firem byla ověřena jejich existence z webových stránek firmy a z obchodního rejstříku tak, aby sestavovaný seznam obsahoval co nejaktuálnější informace ke dni zpracování. Zdroje, které byly postupně procházeny a z nichž byly firmy zahrnuty do seznamu, jsou uvedeny níže v pořadí, jak byly využity.

- České firmy uvedené v EU Civil Security Stakeholder catalogue, který je přílohou studie EU security market study Evropské komise – https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study_en
- Firmy spolupracující na výzkumných projektech na téma bezpečnosti s firmami identifikovanými v EU Civil Security Stakeholder catalogue (viz výše). Zdrojem byl *Informační systém výzkumu, vývoje a inovací*, téma bezpečnosti bylo vymezeno s využitím sady klíčových slov (obecná klíčová slova týkající se oblasti bezpečnosti) nacházejících se v nadpisech a abstraktech řešených projektů.
- Firmy zapojené do alespoň dvou výzkumných projektů zabývajících se oblastí bezpečnosti v letech 2020-2024. Zdrojem byl *Informační systém výzkumu, vývoje a inovací*, téma bezpečnosti bylo vymezeno s využitím sady klíčových slov (detailnější sada klíčových slov v oblasti bezpečnosti než v předchozím kroku) nacházejících se v nadpisech a abstraktech projektů.
- Firmy, které jsou členkami Asociace obranného a bezpečnostního průmyslu České republiky a jsou zařazeny do dílčích oblastí členů *vybavení bezpečnostních služeb* a *obchodní a ostatní*.
- Firmy působící v oblasti kybernetické bezpečnosti doplněné z katalogů Czech Digital Solutions (https://czechdigitalsolutions.cz/cs/organizace/?categories=70861f98-6f0c-409a-8e30-3bcd5fb6206e) a SystemOnLine (https://www.systemonline.cz/dodavatele-it-sluzeb-a-reseni/informacni-bezpecnost/).
- Firmy doplněné pokročilým dotazováním velkého jazykového modelu OpenAI o1-preview (tréninková data aktuální k říjnu 2023).
- Firmy vystavující na veletrhu IDET 2023 dle katalogu vystavovatelů.
- Firmy vystavující na veletrhu PYROS – ISET 2023 dle katalogu vystavovatelů.

Z těchto informačních zdrojů bylo identifikováno celkem 432 podniků. Zastoupení podniků zjištěných z jednotlivých zdrojů ukazuje Obrázek 1.

Obrázek 1 - Zastoupení podniků identifikovaných z jednotlivých informačních zdrojů. Zdroj: vlastní zpracování



Relevance firem oblasti bezpečnostních a obranných technologií, tedy skutečnost, že se identifikované podniky skutečně věnují aktivitám v oblasti bezpečnosti a obrany, byla následně u každého podniku jednotlivě ověřena z jeho webových stránek. Pokud webová prezentace podniku neposkytla jednoznačné informace o jeho zaměření a aktivitách, byly tyto dohledávány dotazováním prostřednictvím vyhledávače Google.

Je potřeba zmínit, že seznam je vždy určitým pohledem v jeden časový okamžik, který se snaží zachytit jinak dynamickou a proměnlivou situaci na trhu. Firmy vznikají a zanikají, fúzují do větších společností v Česku i zahraničí nebo se od nich oddělují. Zda firma působí v Česku lze určit jen nepřímo, třeba pokud zde působí organizační jednotka mateřské zahraniční firmy, ale někdy to určit nelze, zejména v případě akvizic do globálních firem se sídlem v zahraničí a jen s několika málo deklarovanými obchodními pobočkami ve třetích zemích. To znamená, že na českém trhu samozřejmě působí i velké množství zahraničních firem a jejich vztahy k místní výrobě a místním službám či dodavatelským řetězcům lze zjišťovat jen v omezeném rozsahu. Pro zařazení do seznamu tak bylo rozhodující, zda firma má v Česku nějakou organizační jednotku v obchodním rejstříku.

U všech firem zařazených do seznamu byly dále doplněny dodatečné informace:

- Kategorie počtu zaměstnanců z Rejstříku ekonomických subjektů.
- Údaj o objemu finančního plnění za veřejné zakázky, které firma realizovala v období 2020-2024, zdrojem byl Registr smluv. Dále byl doplněn orientační údaj o rozlišení finančního plnění za veřejné zakázky v oblasti bezpečnosti (využito filtrování sadou klíčových slov; kvalita údaje se odvíjí od kvality popisek předmětu plnění veřejné zakázky, která je mezi uveřejňujícími subjekty výrazně různá).

Pro všechny firmy byl z českých webových zdrojů sestaven stručný popis aktivit a produktového portfolia, který dále sloužil k orientačnímu zařazení firem do našich předem definovaných čtyř podoblastí bezpečnostního trhu a podoblasti ‚ostatní', do níž byly zařazeny podniky, které svými produkty a účelem jejich využití (dle popisu na internetových stránkách firem) přísluší spíše trhu s obranným (vojenským) materiálem. Do této specifické podoblasti byly zařazeny podniky působící v segmentu letecké techniky, obrněných vozidel a střelných zbraní. Vzhledem k širokému portfoliu produktů sledovaných firem byly některé z nich zařazeny do více podoblastí bezpečnosti. Zařazení podniků do jednotlivých podoblastí dále posloužilo jako východisko pro přesnější analýzu aktivit firem.

Následně byla pro firmy v uvedených čtyřech podoblastech bezpečnosti provedena kvalitativní segmentační analýza, která v jednotlivých podoblastech identifikovala specifické skupiny produktů (výrobků a služeb) poskytovaných analyzovanými firmami. Segmentační analýza byla založena na následující sadě kritérií vztahujících se k aktivitám a produktům podniků:

- Zaměření podniku (vlastní výrobní aktivity, prodej, výzkum a vývoj, vzdělávání a kombinace těchto aktivit);
- Obor činnosti;
- Šíře produktového portfolia;
- Technologické zaměření.

Identifikované segmenty byly blíže charakterizovány podle popisu produktů a aktivit podniků sdružených v daných segmentech. Na základě počtu podniků působících v jednotlivých segmentech stanoven relativní význam segmentů v rámci jednotlivých podoblastí.

Analýza strany poptávky po bezpečnostních a obranných technologiích byla značně limitována dostupností informací o zakázkách v oblasti bezpečnosti a ekonomických ukazatelích podniků, které v této oblasti působí. Ekonomické ukazatele podniků zveřejňované v podobě výkazu zisků a ztrát ve Sbírce listin (a následně přejímaných do komerčních databází podniků), jsou velmi neúplné (pětileté časové řady by bylo možné vytvořit zhruba u 25 % podniků a data ke konkrétnímu roku v rozmezí +- jednoho roku jsou dostupná přibližně pro 40 % podniků), a tedy obtížně využitelné pro analýzy časových řad i pro průřezové analýzy, podle nichž by bylo možné hodnotit vývoj a velikost tržních segmentů. Z informací o zakázkách podniků jsou dostupné jen informace o veřejných zakázkách, informace o mezifiremních zakázkách nejsou nikde systematicky zveřejňovány, a to zpravidla ani ve výročních zprávách podniků.

Proto byly pro analýzu strany poptávky využity jen informace o veřejných zakázkách v oblasti bezpečnostních a obranných technologiích, které jsou uvedeny v Registru smluv. Objem veřejných zakázek byl sledován pro období 2020-2024 a na úrovni jednotlivých oblastí bezpečnosti a identifikovaných segmentů. Nicméně i tento způsob hodnocení čelí metodologickým nedostatkům. V prvé řadě v tomto registru nejsou uvedeny veřejné zakázky s utajovaným obsahem. Další nedostatek spočívá v relativně krátkém (pětiletém) období sledování objemu veřejných zakázek. Byly sledovány jen zakázky uzavřené v tomto období (resp. celkový objem veřejných zakázek uzavřených v tomto období), nikoliv zakázky uzavřené v předchozím období, jejichž délka plnění přesahovala do sledovaného období.

Charakteristiku hlavních segmentů v jednotlivých podoblastech doplňují stručné popisy vybraných podniků, které byly zařazeny do daných segmentů. Podniky byly vybrány podle objemu veřejných zakázek, které získaly v oblasti bezpečnosti, a zaměření svých produktů, resp. dodávaných technologií.

3 Základní charakteristika podniků v oblasti bezpečnostních technologií

Z využitých informačních zdrojů bylo identifikováno 432 podniků, které působí v oblasti bezpečnostních a obranných technologií. Převládají mezi nimi malé podniky (do 50 zaměstnanců), jejich podíl na celkovém počtu podniků dosahuje 49,3 % (tj. 213 podniků). Následují středně velké podniky (50-249 zaměstnanců) s 27,7% podílem (120 podniků) a velké podniky (nad 250 zaměstnanců) se 14% podílem (61 podniků). U 8,8 % podniků se nepodařilo zjistit jejich velikost.

Tabulka 1 ukazuje podrobnější členění velikostní struktury podniků. Nejvíce podniků přísluší velikostním kategoriím 25-49 zaměstnanců (14,8 %), 100-199 zaměstnanců (13,2 %), 1-5 zaměstnanců (11,3 %), 10-19 zaměstnanců (11,1 %) a 50-99 zaměstnanců (11,1 %).

Tabulka 1 - Počet podniků a objem veřejných zakázek v oblasti bezpečnostních a obranných technologií dle velikostních kategorií podniků. Zdroj: vlastní zpracování

	Firmy		Objem zakázek	
velikostní kategorie	Počet	%	Kč	%
1 - 5 zaměstnanců	49	11,34	15 079 862,46	0,15
6 - 9 zaměstnanců	28	6,48	40 946 890,93	0,41
10 - 19 zaměstnanců	48	11,11	97 113 185,79	0,97
20 - 24 zaměstnanci	24	5,56	232 828 561,72	2,33
25 - 49 zaměstnanců	64	14,81	776 643 727,33	7,77
50 - 99 zaměstnanců	48	11,11	793 649 822,73	7,94
100 - 199 zaměstnanců	57	13,19	1 839 413 395,37	18,41
200 - 249 zaměstnanců	15	3,47	71 804 870,45	0,72
250 - 499 zaměstnanců	30	6,94	1 961 024 123,58	19,63
500 - 999 zaměstnanců	15	3,47	3 421 024 046,00	34,24
1000 - 1499 zaměstnanců	7	1,62	49 106 499,83	0,49
1500 - 1999 zaměstnanců	6	1,39	397 511 082,73	3,98
2000 - 2499 zaměstnanců	1	0,23	3 968 017,00	0,04
5000 - 9999 zaměstnanců	2	0,46	288 657 740,81	2,89
Neuvedeno	38	8,80	1 836 062,39	0,02
Celkem	**432**	**100,00**	**9 990 607 889,12**	**100,00**

Identifikované podniky získaly téměř 10 mld. Kč z veřejných zakázek, které směřovaly do oblasti bezpečnostních a obranných technologií. Největší objem těchto zakázek připadl velkým podnikům (přibližně 6 mld. Kč, tedy 61,3 % z celkového objemu), nejméně obdržely malé podniky (1,16 mld. Kč, 11,6 %).

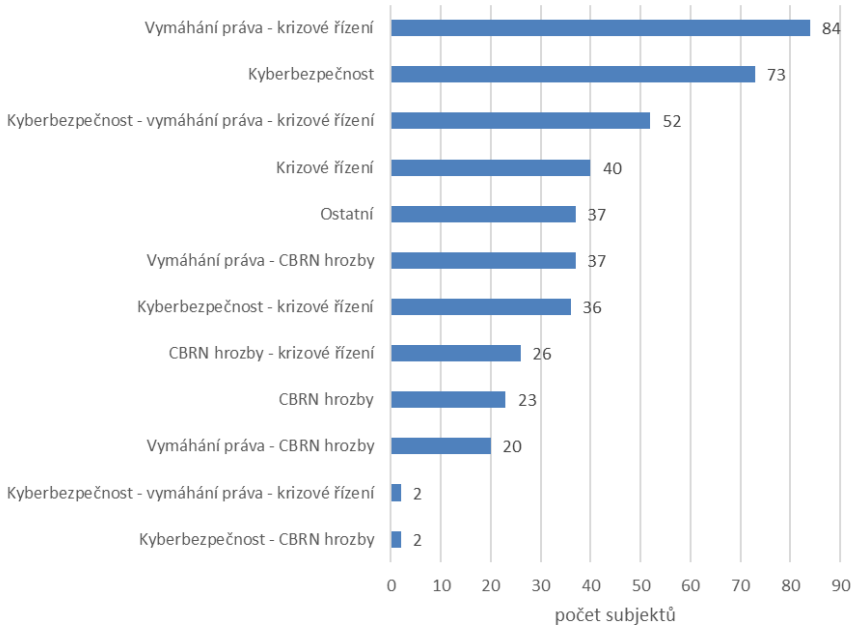
Podrobnější přehled distribuce objemu veřejných zakázek v oblasti bezpečnostních a obranných technologií dle velikostních kategorií podniků přináší Tabulka 1. Objem veřejných zakázek je mezi velikostními kategoriemi podniků i mezi podniky výrazně asymetricky rozložen. Přibližně 54 % objemu se koncentruje ve dvou velikostních kategoriích podniků. Největší objem veřejných zakázek v oblasti bezpečnostních a obranných technologií, a to 3,42 mld. Kč (34,24 % z celkového objemu veřejných zakázek v oblasti bezpečnostních a obranných technologií), získaly podniky z velikostní kategorie 500-999 zaměstnanců. Druhou velikostní kategorii s nejvyšším objemem veřejných zakázek představují podniky s 250-199 zaměstnanci, které obdržely 1,96 mld. Kč (19,63 %).

51 % objemu veřejných zakázek získalo pouze 5 podniků (tedy 1,16 % podniků), 10 podniků obdrželo 68 % objemu zakázek. Naopak 237 podniků (54,9 % podniků) nezískalo žádnou veřejnou zakázku v oblasti bezpečnostních technologií.

Vzhledem k širokému portfoliu produktů (výrobků a služeb), které tyto podniky poskytují, 222 podniků (51,4 % z celkového počtu podniků) působilo ve více oblastech bezpečnosti. Kombinace oblastí, v nichž podniky působí, ukazuje Obrázek 2. V jediné oblasti působilo 210 podniků. Z podniků, které působily v jediné oblasti, jich je nejvíce v oblasti kybernetické bezpečnosti (73 podniků, 34,8 % podniků, které

působily v jediné oblasti a 16,9 % z celkového počtu podniků), dále v oblasti krizového řízení (40 podniků, 19 % z podniků působících v jediné oblasti, 9,3 % z celkového počtu podniků) a vymáhání práva (37 podniků, 17,6 %, resp. 8,7 %). V případě kombinací oborů nejvíce firem působilo v oblasti krizového řízení a současně vymáhání práva (84 podniků, 18,9 % podniků působících ve více oborech, 9,7 % ze všech podniků).

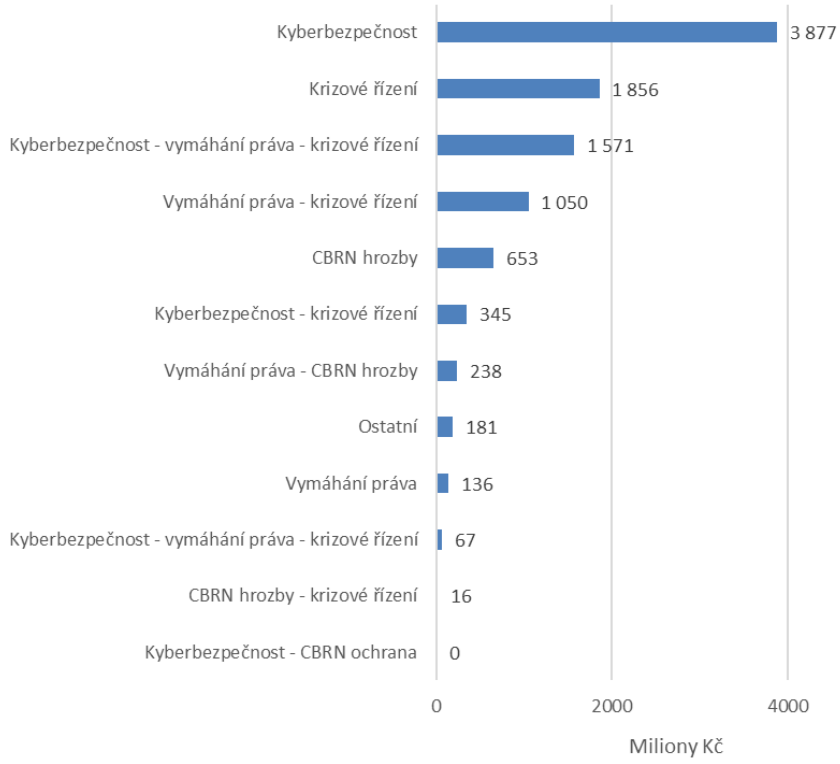
Obrázek 2 - Počet podniků působících v kombinacích oblastí bezpečnosti. Zdroj: vlastní zpracování



Působení více než poloviny podniků ve více oblastech bezpečnosti limituje možnost rozdělit objem veřejných zakázek v oblasti bezpečnostních technologií do jednotlivých oblastí bezpečnosti. Veřejné zakázky se zpravidla vztahují k technologiím v určitém oboru. Jejich přiřazení dle oborů, v nichž podniky působí, by u firem, jejichž aktivity přesahují do více oborů, bylo velmi zkreslující a mohlo by vést k nesprávnému přiřazení. Z tohoto důvodu je možné sledovat jen objem veřejných zakázek realizovaných podniky působících v dané oblasti či v jednotlivých kombinacích oblastí bezpečnosti, nikoliv celkovou oborovou strukturu veřejných zakázek.

Objem veřejných zakázek dle kombinace oblastí bezpečnosti, v nichž působí identifikované podniky, ukazuje Obrázek 3. Nejvyšší objem veřejných zakázek realizovaly podniky v oblasti kybernetické bezpečnosti (3,88 mld. Kč, 38,8 % z celkového objemu zakázek v oblasti bezpečnostních technologií) a krizového řízení (1,856 mld. Kč, 18,6 % z celkového objemu zakázek v oblasti bezpečnostních technologií). Následují podniky působící v kombinaci oblasti kybernetické bezpečnosti, vymáhání práva a krizového řízení, které obdržely 1,571 mld. Kč, tedy 15,7 %).

Obrázek 3 - Objem veřejných zakázek (v Kč) dle oblastí a kombinace oblastí bezpečnosti. Zdroj: vlastní zpracování



4 Popis oblastí

4.1 Kybernetická bezpečnost

Dle použitých informačních zdrojů v oblasti kybernetické bezpečnosti působí 117 subjektů. Nejvíce z těchto podniků (51,3 %) se svojí velikostí řadí mezi malé podniky. Středně velké podniky se na celkovém počtu těchto subjektů podílejí přibližně čtvrtinou (26,5 %) a velké podniky přibližně jednou sedminou (14,5 %). U zbývajícího počtu podniků není uvedena velikostní kategorie. Podrobnější členění velikostní struktury ukazuje Tabulka 2. Nejvíce zastoupeny jsou podniky s 50-99 zaměstnanci (17 podniků), 25-49 zaměstnanci (16 podniků), 10-19 zaměstnanci (15 podniků) a 1-5 zaměstnanci (15 podniků).

Tabulka 2 - Počet podniků a objem veřejných zakázek podniků působících v oblasti kyberbezpečnosti podle velikostních kategorií podniků. Zdroj: vlastní zpracování

		Subjekty		Veřejné zakázky	
Kategorie podniku	**Počet zaměstnanců**	**Počet**	**%**	**Objem v Kč**	**%**
	1 - 5	15	12,82	12 549 849	0,21
	6 - 9	7	5,98	40 407 607	0,67
	10 - 19	15	12,82	37 937 559	0,63
	20 - 24	7	5,98	34 982 329	0,58
Malé	25 - 49	16	13,68	560 537 203	9,28
	50 - 99	17	14,53	669 730 698	11,08
	100 - 199	12	10,26	638 193 944	10,56
Střední	200 - 249	2	1,71	12 016 873	0,20
	250 - 499	10	8,55	1 174 393 057	19,44
	500 - 999	4	3,42	2 852 038 069	47,20
	1000 - 1499	1	0,85	293 627	0,00
	1500 - 1999	1	0,85	0	0,00
Velké	5000 - 9999	1	0,85	7 679 692	0,13
Neuvedeno		9	7,69	1 131 600	0,02
Celkem		**117**	**100,00**	**6 041 892 108**	**100,00**

Veřejné zakázky v oblasti bezpečnostních technologií získalo 70 subjektů (tedy 59,8 % z celkového počtu podniků podnikajících v oblasti kybernetické bezpečnosti). Velikostní strukturu podniků a objem získaných zakázek přibližuje Tabulka 2. Z ní je zejména zřejmé krajně nerovnoměrné rozložení objemu veřejných zakázek, 47 % objemu veřejných zakázek příslušelo firmám z velikostní kategorie 500-999 zaměstnanců a 19,4 % firmám s 250-499 zaměstnanci.

Na základě zaměření dodávaných produktů (výrobků a služeb) byly subjekty působící v oblasti kybernetické bezpečnosti rozděleny do následujících specifických tematických skupin:

- Prevence kyberkriminality a řešení kybernetické bezpečnosti;
- Digitální transformace a IT poradenství;
- Digitální forenzní analýza;
- Kybernetická bezpečnost kritické infrastruktury;
- Kybernetická bezpečnost v krizovém řízení;
- Řešení pro správu identit a ověřování;
- Výzkum a vývoj v oblasti kybernetické bezpečnosti.

Celkový počet subjektů podnikajících v těchto tematických skupinách včetně počtu subjektů podnikajících pouze v těchto skupinách ukazuje Tabulka 3. Nejvíce podniků (40,17 %) působilo v tematické skupině *Prevence kyberkriminality a řešení kybernetické bezpečnosti*. Téměř čtvrtina

podniků se věnuje tématu *Digitální transformace a IT poradenství*. Třetí nejvíce zastoupenou tematickou oblastí je *Digitální forenzní analýza*, jíž se věnuje 12,82 % podniků.

U 37,61 % podniků jejich aktivity zahrnují i jiné oblasti než kybernetickou bezpečnost, zatímco 62,39 % podniků působí pouze v oblasti kyberbezpečnosti, jak je zřejmé z Tabulka 3. Tyto podniky dominují v tematických skupinách *Digitální transformace a IT poradenství, Výzkum a vývoj v oblasti kyberbezpečnosti, Prevence kyberkriminality a řešení kybernetické bezpečnosti* a *Řešení pro správu identit a ověřování*. Podniky, které se věnují i jiným oblastem než kybernetické bezpečnosti, převládají v tematických skupinách *Digitální forenzní analýza, Kybernetická bezpečnost kritické infrastruktury* a *Kybernetická bezpečnost pro krizové řízení*. Zaměřením svých produktů přesahují do oblastí vymáhání práva a krizového řízení.

Tabulka 3 - Celkový počet podniků a počet podniků působících pouze v oblasti kyberbezpečnosti podle tematických skupin. Zdroj: vlastní zpracování

Skupina	Subjekty celkem		Subjekty jen v oboru kyberbezpečnosti		
	Počet	%	Počet	%	Podíl na celkovém počtu subjektů v oblasti kyberbezpečnosti (v %)
Prevence kyberkriminality a a řešení kybernetické bezpečnosti	47	40,17	35	47,95	74,47
Digitální transformace a IT poradenství	29	24,79	25	34,25	86,21
Digitální forenzní analýza	15	12,82	4	5,48	26,67
Kybernetická bezpečnost kritické infrastruktury	9	7,69	2	2,74	22,22
Kybernetická bezpečnost v krizovém řízení	8	6,84	1	1,37	12,50
Řešení pro správu identit a ověřování	5	4,27	3	4,11	60,00
Výzkum a vývoj v oblasti kyberbezpečnosti	4	3,42	3	4,11	75,00
Celkem	**117**	**100,00**	**73**	**100,00**	**62,39**

Více než 40 % objemu veřejných zakázek je alokováno v tematické skupině *Digitální transformace a IT poradenství* (viz Tabulka 4). Zhruba poloviční hodnoty dosahuje objem veřejných zakázek u dalších tematických skupin – *Kybernetická bezpečnost kritické infrastruktury* (20,46 %) a *Digitální forenzní analýza* (19,26 %).

Tabulka 4 - Objem veřejných zakázek v tematických skupinách kyberbezpečnosti. Zdroj: vlastní zpracování

Skupina	Veřejné zakázky celkem		Veřejné zakázky podniků působících jen v oblasti kyberbezpečnosti		
	Kč	%	Kč	%	Podíl na celkovém objemu veřejných zakázek (v %)
Digitální transformace a IT poradenství	2 556 723 451	42,32	2 544 574 019	65,63	99,52
Kybernetická bezpečnost kritické infrastruktury	1 236 324 189	20,46	958 117 082	24,71	77,50
Digitální forenzní analýza	1 163 923 565	19,26	2 601 000	0,07	0,22
Prevence kyberkriminality a a řešení kybernetické bezpečnosti	707 683 928	11,71	296 184 916	7,64	41,85
Kybernetická bezpečnost v krizovém řízení	299 031 528	4,95	0	0,00	0,00
Výzkum a vývoj v oblasti kyberbezpečnosti	63 867 296	1,06	63 676 116	1,64	99,70
Řešení pro správu identit a ověřování	14 338 150	0,24	12 073 030	0,31	84,20
Celkem	**6 041 892 108**	**100,00**	**3 877 226 163**	**100,00**	**64,17**

Níže jsou stručně charakterizovány jednotlivé tematické skupiny podniků.

Prevence kyberkriminality a řešení kybernetické bezpečnosti

- Komplexní řešení kybernetické bezpečnosti – komplexní řešení, která řeší více aspektů kybernetické bezpečnosti, například správu infrastruktury, zabezpečení cloudu, zabezpečení sítě a správu identit.

- Zabezpečení sítě a ochrana infrastruktury – ochrana před síťovými kybernetickými útoky prostřednictvím technologií jako jsou firewally, VPN, systémy detekce sítí a reakce na ně.
- Audity kybernetické bezpečnosti, penetrační testování a reakce na incidenty – identifikace zranitelných míst, simulace útoků a reakce na bezpečnostní incidenty s cílem posílit bezpečnostní pozici svých klientů.
- Zabezpečení cloudu a IT infrastruktury – řešení kybernetické bezpečnosti speciálně pro cloudová prostředí a IT infrastrukturu (bezpečný cloudový hosting, ochranu dat, monitorování hrozeb a soulad s průmyslovými normami).
- Prevence kyberkriminality pomocí umělé inteligence a strojového učení – využití umělé inteligence a strojového učení k odhalování a prevenci kybernetických hrozeb v reálném čase (zejména v oblasti detekce podvodů, identifikace malwaru a analýzy chování).
- Zabezpečená komunikace a ochrana dat – šifrovaná komunikační řešení, služby bezpečného přenosu dat a pokročilé systémy prevence ztráty dat.
- Vývoj softwaru na zakázku a bezpečnostní integrace – vývoj softwaru na zakázku s integrovanými bezpečnostními prvky.
- Školení a vzdělávání v oblasti kybernetické bezpečnosti – vzdělávání a školení odborníků v oblasti kybernetické bezpečnosti.

Příklady podniků, které působí v této tematické skupině přináší Rámeček 1 a Rámeček 2.

Rámeček 1 - ANECT a.s. Zdroj: https://www.anect.com/

ANECT a.s. je českou společností, která se specializuje na služby v oblasti ICT bezpečnosti, zejména na služby v oblasti hybridních a cloudových řešení pro velké korporace a veřejný sektor. Provozuje čtyři pobočky v ČR a na Slovensku, v nichž pracuje zhruba 160 zaměstnanců. Kromě domácího trhu dodává také do USA, Německa, Thajska, Číny a dalších zemí. Provozuje také inovační centrum, které vyvíjí vlastní bezpečnostní řešení.

Klíčovým produktem v oblasti kyberbezpečnosti je SOCA (Security Operations Center as a Service), což je služba zajišťující monitorování, detekci a reakci na kybernetické hrozby v reálném čase. Tento produkt je nabízen ve třech variantách: od základního monitoringu až po plně řízené zabezpečení, které zahrnuje nepřetržitý dohled nad IT infrastrukturou, reakci na útoky a následnou analýzu incidentů.

Dalším produktem jsou služby Red Teamingu a penetračních testů, které simulují kybernetické útoky s cílem odhalit slabiny v bezpečnostních opatřeních klienta. Kromě technických testů zahrnují i metody sociálního inženýrství, jako jsou phishingové kampaně a simulace sociálního hackingu, které pomáhají organizacím zvýšit odolnost proti sofistikovaným útokům.

Rámeček 2 - VISITECH a.s. Zdroj: https://www.visitech.cz/

Visitech a.s. byla založená v České republice. Zaměřuje se na poskytování řešení v oblasti ICT infrastruktury a služeb kybernetické bezpečnosti. Mezi její hlavní aktivity patří distribuce IT komponentů a implementace podnikových softwarových řešení zaměřených na ochranu dat a zabezpečení provozních systémů. Firma působí zejména v různých průmyslových odvětvích, kde je bezpečnost dat klíčová kvůli specifickým rizikům spojeným s průmyslovými procesy.

V oblasti kybernetické bezpečnosti se Visitech specializuje na ochranu podnikové infrastruktury před kybernetickými hrozbami a na automatizaci bezpečnostních procesů. To zahrnuje implementaci systémů pro detekci a prevenci bezpečnostních incidentů, čímž pomáhá organizacím minimalizovat riziko úniků dat a kybernetických útoků. Jednou z klíčových technologií, kterou společnost nabízí, je její

bezpečnostní informační a řídicí systém, který integruje různé bezpečnostní protokoly a zajišťuje nepřetržitou ochranu kritických systémů.

Klíčovým produktem je centrum kybernetické bezpečnosti – Security Operation Center SOC365 pro správu a dohled ICT sítí. V jeho rámci je zajišťován Audit ICT, PIM/PAM, penetrační testy, Endpoint Security a Firewall, Mobile device management, Šifrování e-mailů a dokumentů, Bezpečný archiv a Data Loss Prevention, Monitoring sítí a aplikací, Centrální správa IP adresního prostoru či Log Management Systém.

Vymáhání práva a digitální forenzní analýza

- Digitální forenzní a vyšetřovací nástroje – vývoj forenzních nástrojů a řešení pro forenzní analýzu mobilních zařízení, forenzní analýzu kryptoměnových transakcí a obnovu dat.
- Řešení kybernetické bezpečnosti pro orgány činné v trestním řízení – zabezpečení kritických informačních systémů, zřizování bezpečnostních operačních center (SOC), poskytování služeb reakce na incidenty a nasazování systémů dohledu a kontroly přístupu k ochraně utajovaných a citlivých informací.
- Biometrická řešení a umělá inteligence pro vymáhání práva – pokročilá biometrická řešení a řešení AI, která pomáhají orgánům činným v trestním řízení při identifikaci podezřelých osob a zajišťování důkazů (systémy rozpoznávání obličeje, analýzy hlasu a identifikace na bázi umělé inteligence, které se používají v bezpečnostních aplikacích a při vyšetřování).
- Forenzní datová analýza a zpravodajská řešení – forenzní analýza dat a zpravodajská řešení, která umožňují orgánům činným v trestním řízení analyzovat velké objemy dat (identifikace zločineckých sítí a hrozeb pomocí analýzy dat, shromažďování zpravodajských informací a technik dolování dat, které umožňují řešit složité případy kyberkriminality).
- Kryptografické systémy a bezpečná komunikace pro orgány činné v trestním řízení – kryptografické systémy, platformy pro bezpečné sdílení informací a pokročilé komunikační technologie.
- Prevence a výzkum kyberkriminality – výzkum a vývoj inovativních řešení pro prevenci kyberkriminality (umělá inteligence, strojové učení a velké objemy dat apod.).

Příklady podniků, které působí v této tematické skupině přináší Rámeček 3.

Rámeček 3 - Netsearch s.r.o. Zdroj: https://www.netsearch.cz/

Netsearch s.r.o. se specializuje na kybernetickou bezpečnost a digitální forenzní technologie. Své služby poskytuje zejména organizacím veřejného a finančního sektoru. Vyvíjí pokročilé softwarové a hardwarové nástroje pro analýzu kybernetických hrozeb, přičemž se zaměřuje zejména na analýzu kryptoměn, obnovu hesel a sledování síťového provozu.

K jejím klíčovým produktům patří systém COINØMON, který provádí forenzní analýzu blockchainů a sledování podezřelých transakcí, čímž pomáhá odhalovat praní špinavých peněz a sledovat pohyb nelegálních finančních prostředků.

Dalším produktem je DEFRAUDify, což je platforma zaměřená na identifikaci podvodných aktivit na tzv. darknetu a běžném webu. Tento produkt kombinuje různé nástroje pro automatizované sledování a identifikaci a analýzu podvodných transakcí.

Produkt PASSVORTO je nástrojem pro analýzu úniků hesel a osobních údajů, který firmám umožňuje rychle identifikovat kompromitované účty a přijímat opatření k ochraně citlivých dat. Další produkt, ORWELL, je nástrojem pro shromažďování důkazů schopný pokročilého, parametrizovaného

procházení a archivace webových stránek. Umožňuje shromažďovat a z různých zdrojů (např. surface web, deep web, dark web) získávat online důkazy o nezákonných aktivitách.

Digitální transformace a IT poradenství

- Poradenství v oblasti kybernetické bezpečnosti – pokročilé poradenské služby v oblasti kybernetické bezpečnosti (řízení rizik, reakce na incidenty, penetrační testování a audity kybernetické bezpečnosti, zejména pro kritickou infrastrukturu).
- Komplexní digitální transformace a IT služby – služby digitální transformace, které často zahrnují IT poradenství, systémovou integraci, cloud computing, DevOps a kybernetickou bezpečnost
- Poskytovatelé cloudové infrastruktury a zabezpečení – služby cloudové infrastruktury a zabezpečení s důrazem na ochranu dat, bezpečné cloudové prostředí a zabezpečení sítě (řešení pro správu bezpečnostních rizik v prostředí cloud computingu, včetně bezpečných sítí VPN, šifrování dat a monitorování hrozeb).
- Vývoj softwaru na zakázku a automatizace s kybernetickou bezpečností – vývoj softwaru na míru, který zahrnuje kybernetickou bezpečnost jako základní součást (automatizace podnikových procesů, vývoj aplikací AI a IoT a zajištění bezpečných softwarových řešení).
- Správa IT infrastruktury a služby kybernetické bezpečnosti – správa IT infrastruktury a zajištění její bezpečnosti (správa datových center, zabezpečení sítí a bezpečné komunikační systémy).
- Řešení pro elektronickou veřejnou správu a bezpečnost ve veřejném sektoru – bezpečná správa identit, elektronické podepisování dokumentů a systémy určené k zajištění souladu s právními předpisy ve veřejném sektoru.
- Řešení proti sledování a specializovaná řešení kybernetické bezpečnosti – pokročilá řešení kybernetické bezpečnosti se zaměřením na ochranu proti sledování, bezpečnou komunikaci a ochranu citlivých prostředí (technologie pro detekci a neutralizaci sledovacích zařízení a zabezpečení komunikačních kanálů).
- Řízení projektů, audity a dodržování předpisů v oblasti kybernetické bezpečnosti – audity GDPR, hodnocení rizik a zajištění toho, aby kybernetická bezpečnost byla nedílnou součástí řízení podniku a pracovních postupů projektů.

Příklady podniků, které působí v této tematické skupině přináší Rámeček 4 a Rámeček 5.

Rámeček 4 - Aricoma Systems a.s. Zdroj: https://www.aricoma.com/cs/home

Aricoma Systems a.s. patří ve střední Evropě mezi klíčové hráče v oblasti kybernetické bezpečnosti. Na trhu působí již více než 30let. Její služby zahrnují komplexní správu bezpečnostních incidentů, penetrační testování, správu zranitelnosti, ochranu koncových bodů (EDR), správu identit a vzdělávání zaměstnanců. Také provozuje vlastní inovační laboratoř, kde vyvíjí a testuje nové bezpečnostní technologie.

Hlavním produktem je tzv. Red Teaming (penetrační testy), který simuluje reálné útoky a pomáhá organizacím odhalit zranitelná místa jejich systémů a procesů. Red Team se zaměřuje nejen na technickou stránku, ale i na fyzickou a psychologickou bezpečnost, využívá přitom různé techniky sociálního inženýrství, jako je například klonování přístupových karet nebo phishing. Cílem těchto simulací je testovat připravenost obranných týmů zákazníků (Blue Team) a umožnit jim lépe identifikovat a zastavit podobné hrozby v budoucnu.

Mezi hlavní aktivity této společnosti dále patří:

- Bezpečnostní dohled formou služby – komplexní bezpečnostní dohled (SOC), řešení XDR formou služby (XDRSaaS) reakce na incidenty formou služby (IRaaS, CSIRT), správa zranitelností formou služby (VMSaaS), ochrana značky formou služby (DRPaaS).
- Správa bezpečnostních informací.
- Správa logů a bezpečnostních událostí (SEM) - komplexní systémy řízení bezpečnosti (SIEM).
- Řízení rizik a soulad s předpisy – systémy pro automatizaci řízení rizik (GRC, IRM), analýza rizik, implementace ISMS, dodržování shody (GDPR, NIS2, ZoKB, audity), řízení kontinuity činností (BCM, BIA, DRP), krizové řízení.
- Bezpečnost IT infrastruktury a cloudu – ochrana koncových zařízení (EDR, EPP), řešení pro rozšířenou detekci a reakci (XDR), síťová ochrana (VPN, FW, GW, SD-WAN), řízení síťových přístupů (NAC, NDR), bezpečnost cloud prostředí (CASB, API Security), ochrana DNS, řízení zranitelností (VMS), hardening systémů, bezpečnost technologických sítí (OT), správa digitálních hrozeb (EASM, TI, ochrana značky).
- Správa identit a přístupů – řízení identit (IDM, AD, LDAP), řízení přístupu (PKI, MFA, SSO), řízení privilegovaných přístupů (PIM/PAM).
- Ochrana dat – klasifikace informací a dokumentů, ochrana informací (AIP), ochrana před únikem dat (DLP), šifrování dat.
- Systémová a aplikační bezpečnost – zálohování, replikace a obnova dat, webový aplikační firewall (WAF), LoadBalancing řešení, automatizované platformy pro ověřování zabezpečení.

Rámeček 5 - UNIS COMPUTERS, a.s. Zdroj: https://www.uniscomp.cz/

UNIS COMPUTERS, a.s. je poskytovatelem IT a kyberbezpečnostních řešení s více než 28letými zkušenostmi. Specializuje se na komplexní služby počínaje návrhem, dodávkami a instalací serverů, datových úložišť, aktivních síťových prvků či síťových operačních systémů až po servisní služby. Důraz klade na bezpečnost dat a ochranu před kybernetickými hrozbami. Své služby poskytuje jak podnikovému sektoru, tak také veřejným institucím včetně nemocnic, univerzit apod.

V oblasti kyberbezpečnosti nabízí služby jako audity zabezpečení, posuzování souladu s předpisy GDPR, a řízení přístupu k síti. Provádí podrobné audity, které zahrnují kontrolu organizačních a technických opatření, zajišťují ochranu infrastruktury před útoky, správu bezpečnostních politik a dohled nad incidenty. Také se věnuje ochraně perimetru sítí LAN a WLAN, zajišťování bezpečné autentizace uživatelů a kontrole přístupu k datovým zdrojům.

Nabízí jednorázové i dlouhodobé služby. Jednorázové služby zahrnují jednorázový bezpečnostní audit IT, návrhy účinného zabezpečení IT, návrhy zabezpečení objektů – kamerovými systémy a elektronickými zabezpečovacími systémy a realizaci zabezpečení objektů. Mezi dlouhodobé služby patří realizace účinného zabezpečení IT a stálý dohled spočívající (i.) v zajištění firewallu, VPN, antivirovém a antispamovém zabezpečení, (ii.) a monitoringu zařízení, (iii.) monitoring datových toků a (iv.) managementu bezpečnostních informací a událostí.

Řešení pro správu identit a ověřování

- Platformy pro správu identit a řízení přístupu – platformy pro správu identit, které poskytují řešení pro bezpečné řízení přístupu a ověřování uživatelů.
- Biometrické systémy a bezpečnostní integrace pro orgány činné v trestním řízení – integrace bezpečnostních řešení s biometrickými systémy, jako je rozpoznávání obličeje a snímání otisků prstů.
- Digitální identita a autentizační řešení pro finanční služby – poskytování řešení digitální identity a autentizace na míru pro finanční služby a vládní subjekty (bezpečné elektronické platby,

autentizační systémy a dodržování předpisů o kybernetické bezpečnosti pro ochranu citlivých finančních údajů a identit).

- Komplexní řešení kybernetické bezpečnosti a ochrany dat – komplexní služby kybernetické bezpečnosti zaměřené na ochranu dat a infrastruktury prostřednictvím spravovaných IT a cloudových řešení (včetně správy mobilních zařízení, zabezpečení hybridního cloudu a správy identit a zajištění bezpečné správy a monitorování dat i zařízení uživatelů).

Výzkum, inovace a vzdělávání v oblasti kybernetické bezpečnosti

- Vývoj nových nástrojů, strategií a informovanosti v boji proti kybernetické kriminalitě.

Kybernetická bezpečnost kritické infrastruktury

- Bezpečnost IT a obnova po havárii pro kritickou infrastrukturu – služby v oblasti bezpečnosti IT a obnovy po havárii (ochrana dat, správa serverů a zavádění systémů správy identit).
- Bezpečná komunikace a kybernetická bezpečnost pro kritickou infrastrukturu – bezpečné komunikační technologie a řešení kybernetické bezpečnosti přizpůsobená odvětvím kritické infrastruktury.
- Internet věcí a chytrá řešení pro průmyslové aplikace – integrace technologií internetu věcí do kritické infrastruktury (sběr dat v reálném čase, inteligentní automatizace a lepší provozní řízení).
- Fyzická bezpečnost a nízkonapěťové technologie pro kritickou infrastrukturu – fyzická bezpečnost kritické infrastruktury prostřednictvím nízkonapěťových technologií a integrovaných bezpečnostních systémů (alarmy, kamerové systémy a systémy požární ochrany).
- Řešení pro monitorování infrastruktury a životního prostředí – monitorovací technologie, které v reálném čase poskytují údaje o stavu kritických součástí infrastruktury.

Kybernetická bezpečnost v krizovém řízení

- Bezpečná komunikace a IT řešení pro krizové řízení – poskytování bezpečných komunikačních platforem a IT řešení určených pro krizové řízení a prosazování práva.
- Vysílání, digitální infrastruktura a cloudová řešení pro reakci na mimořádné události – vysílací služby, cloudová infrastruktura a řešení založená na internetu věcí, která podporují kontinuitu kritických služeb během mimořádných událostí.
- Internet věcí a monitorovací technologie pro řízení mimořádných událostí – tyto firmy poskytují monitorovací technologie a řešení internetu věcí, která umožňují sledování kritických prostředků, vozidel a osob v reálném čase během mimořádných událostí.
- Služby technické infrastruktury pro nouzové a telekomunikační potřeby – služby technické a telekomunikační infrastruktury nezbytné pro zachování provozu během mimořádných událostí.
- Krizové řízení a bezpečnostní systémy – řešení pro krizové řízení, která zahrnují nástroje a systémy určené pro zvládání krizových situací, řízení hrozeb a rychlou reakci na fyzické i kybernetické incidenty.

4.2 Krizové řízení

V oblasti krizového řízení podniká dle použitých informačních zdrojů 110 subjektů. Téměř polovina z nich (45,5 %) na základě počtu zaměstnanců přísluší mezi malé podniky a třetina (33,6 %) mezi podniky střední velikosti. Podíl velkých podniků na celkovém počtu subjektů v této oblasti dosahuje 14,5 %). Z Tabulka 5, která ukazuje podrobnější členění velikostní struktury podniků, je zřejmé, že nejvíce subjektů (20 %) má mezi 100-199 zaměstnanci, dále mezi 25-49 zaměstnanci (15,45 %) a 10-19 zaměstnanci (10,91 %). Nejnižší počty podniků jsou v kategoriích s nejvyšším počtem zaměstnanců.

Tabulka 5 - Počet podniků a objem veřejných zakázek podniků působících v oblasti krizového řízení podle velikostních kategorií podniků. Zdroj: vlastní zpracování

		Subjekty		Veřejné zakázky	
Kategorie podniku	**Počet zaměstnanců**	**Počet**	**%**	**Objem v Kč**	**%**
	1 - 5	8	7,27	2 937 668	0,10
	6 - 9	8	7,27	297 284	0,01
	10 - 19	12	10,91	29 800 484	1,05
	20 - 24	5	4,55	34 558 481	1,21
Malé	25 - 49	17	15,45	214 944 981	7,55
	50 - 99	12	10,91	25 401 896	0,89
	100 - 199	22	20,00	1 313 315 466	46,14
Střední	200 - 249	3	2,73	69 863 736	2,45
	250 - 499	10	9,09	715 727 084	25,14
	1000 - 1499	3	2,73	42 898 570	1,51
	1500 - 1999	2	1,82	388 388 832	13,64
Velké	5000 - 9999	1	0,91	7 679 692	0,27
Neuvedeno		7	6,36	704 462	0,02
Celkem		**110**	**100,00**	**2 846 518 638**	**100,00**

Distribuce objemu veřejných zakázek mezi velikostní kategorie podniků je značně nerovnoměrná, jak ukazuje tabulka. Nejvyšší objem veřejných zakázek (více než 1,3 mld. Kč, tedy 46,14 % objemu veřejných zakázek) získaly firmy z početně nejvíce zastoupené velikostní kategorie 100-199 zaměstnanců. Objem veřejných zakázek, které získaly ostatní velikostní kategorie podniků, je významně nižší. Druhá velikostní kategorie s nejvyšším objemem zakázek – 250-499 zaměstnanců – získala 716 mil. Kč (tj. 25,14 %) a třetí – 1500–1999 zaměstnanců 388 mil. Kč (13,64 %).

Subjekty byly na základě specifického zaměření svých produktů a jejich užití rozděleny do následujících tematických skupin:

- Nouzové a záchranné vybavení;
- Komunikační a koordinační (IT) systémy;
- Dohledové a bezpečnostní systémy;
- Radarové systémy;
- Ochrana kritické infrastruktury.

Nejvíce subjektů (41,82 %, tj. 46 subjektů) působí v tematické skupině *Nouzové a záchranné vybavení* a dále ve skupině *Komunikační a koordinační (IT) systémy* (30 %, 33 subjektů). Nejméně subjektů (5, tedy 4,55 %) se specializuje na téma *Ochrana kritické infrastruktury* (viz Tabulka 6). Podniky působící pouze v oblasti krizového řízení převažují v nejméně zastoupené tematické skupině *Ochrana kritické infrastruktury* (60 % podniků, které se věnují tomuto tématu, působí pouze v oblasti krizového řízení), což ovšem může být způsobeno právě malou četností podniků v tomto tématu. U ostatních témat převažují podniky, které současně působí i v jiných oblastech (viz Tabulka 6) Nejvyššího podílu tyto podniky dosahují v tematických skupinách *Radarové systémy* a *Dohledové a bezpečnostní systémy*.

V těchto tematických skupinách působí mimo oblast krizového řízení 85,71 %, resp. 78,95 % podniků, tyto podniky působí současně v oblasti vymáhání práva.

Tabulka 6 - Celkový počet podniků a počet podniků působících pouze v oblasti krizového řízení podle tematických skupin. Zdroj: vlastní zpracování

	Subjekty celkem		Subjekty jen v oblasti krizového řízení		
Skupina	Počet	%	Počet	%	Podíl na celkovém počtu subjektů v oblasti krizového řízení (v %)
Nouzové a záchranné vybavení	46	41,82	19	51,35	41,30
Komunikační a koordinační (IT) systémy	33	30,00	10	27,03	30,30
Dohledové a bezpečnostní systémy	19	17,27	4	10,81	21,05
Radarové systémy	7	6,36	1	2,70	14,29
Ochrana kritické infrastruktury	5	4,55	3	8,11	60,00
Celkem	**110**	**100,00**	**37**	**100,00**	**33,64**

Nejvyšší objemy veřejných zakázek získaly podniky působící v tematických skupinách *Komunikační a koordinační (IT) systémy* (1,7 mld. Kč, 58,94 %) a *Dohledové a bezpečnostní systémy* (919 mil. Kč, tedy 32,29 % objemu veřejných zakázek v oblasti krizového řízení), jak ukazuje Tabulka 7.

Tabulka 7 - Objem veřejných zakázek v tematických skupinách krizového řízení. Zdroj: vlastní zpracování

	Veřejné zakázky celkem		Veřejné zakázky podniků působících jen v oblasti krizového řízení		
Skupina	Kč	%	Kč	%	Podíl na celkovém objemu veřejných zakázek (v %)
Nouzové a záchranné vybavení	88 077 290	3,09	29 377 814	25,59	33,35
Komunikační a koordinační (IT) systémy	1 677 760 187	58,94	1 072 749	0,93	0,06
Dohledové a bezpečnostní systémy	919 029 231	32,29	5 145 610	4,48	0,56
Ochrana kritické infrastruktury	113 924 515	4,00	78 212 674	68,12	68,65
Radarové systémy	47 727 415	1,68	1 008 794	0,88	2,11
Celkem	**2 846 518 638**	**100,00**	**114 817 641**	**100,00**	**4,03**

Níže jsou stručně charakterizovány jednotlivé tematické skupiny podniků.

Nouzové a záchranné vybavení

- Modulární konstrukce a infrastruktura – modulární systémy vhodné pro stavbu nouzových přístřešků, polních nemocnic a infrastruktury důležité pro vojenské a civilní použití.
- Osobní ochranné prostředky a oděvy – ochranné prostředky a oděvy určené pro záchranáře a vojenský personál.
- Zdravotnické a bezpečnostní vybavení pro případ nouze – základní zdravotnické vybavení a bezpečnostní řešení pro záchranné týmy.
- Požární bezpečnost a záchranné vybavení – výrobky a systémy určené k prevenci a zdolávání požárů, včetně hasicích přístrojů, hasičských vozidel a záchranářského vybavení.
- Doprava a logistika pro řešení mimořádných událostí – vozidla a přívěsy určené speciálně pro záchranné služby, dále logistické systémy pro krizové situace.
- Drony a sledovací technologie – drony a dohledové technologie pro vyhodnocování katastrof a monitorování.
- Osvětlovací systémy – přenosná osvětlovací technika pro záchranné služby.

- Potraviny a systémy pro zajištění stravování – hotová jídla a vojenské příděly, logistické zajištění stravování.
- Technické služby a podpora – technická podpora, průzkumné, diagnostické a monitorovací služby.

Příklady podniků, které působí v této tematické skupině přináší Rámeček 6 a Rámeček 7.

Rámeček 6 - GUMOTEX a.s. Zdroj: https://www.gumotex.cz

GUMOTEX, a.s. spolu se svými dceřinými společnostmi patří mezi renomované výrobce produktů z pryže a plastů. Divize Coating nabízí širokou škálu gumárenských směsí a povrchově upravených textilních materiálů, které jsou základem pro výrobu speciálních záchranných systémů.

Jedním z hlavních produktů jsou nafukovací stany a haly vytvářející mobilní zázemí pro složky IZS, policie a armády. GUMOTEX vyrábí stany a haly od velikosti 10 až po 50 m² a dodává k nim kompletní sady příslušenství – vytápění, klimatizace, osvětlení, izolace a propojení. Nafukovací stany vyrábí v modulární verzi s variabilní užitnou plochou v základu od 80 do 225 m².

Dalším produktem jsou mobilní dekontaminační stanoviště pro záchranné složky i protichemické jednotky armád při likvidaci havárií způsobených únikem nebezpečných látek a plynů.

Vyrábí také speciální protipovodňové zábrany, a to ve dvou variantách – válcové a s ocelovou konstrukcí. Bariéry se plní vodou, což zajišťuje jejich stabilitu a efektivitu při ochraně proti povodním a přívalovým dešťům. Válcové protipovodňové zábrany jsou dodávány o délce 10 m a průměru 40 a 80 cm. Díky možnosti pyramidového stavění lze ochrannou výšku zábrany navýšit až do 1 m. Dílce zábrany lze spojovat do požadované délky. Ocelové zábrany jsou navrženy pro extrémní namáhání a poskytují ochrannou výšku až 1,3 m.

Dále GUMOTEX vyrábí speciální ochranné obleky pro zásahy v nebezpečném prostředí a přenosné nádrže pro potřeby požárních hasičských zásahů či zadržení kontaminované vody.

Rámeček 7 - THT Polička, s.r.o. Zdroj: https://tht.cz/

THT Polička, s.r.o. je výrobce požárních vozidel a kontejnerů.

V oblasti krizového řízení nabízí THT Polička specializované vybavení, včetně mobilních nádrží a hasicích vozů s vysokou kapacitou, které umožňují rychlé dodávání vody do míst zásahu. Příkladem vozu s vysokou kapacitou je CV 40–T 815-7 10x10.1, který je navržen pro přepravu až 21 000 litrů vody, což umožňuje hašení požárů ve vzdálených nebo těžko přístupných oblastech, případně doplňování zásob vody během delších či rozsáhlých požárních zásahů. Pro operace v náročných podmínkách dodává specializovaná vozidla na podvozcích TATRA, která zvládnou jízdu v těžkém terénu.

THT Polička také zajišťuje výcvik záchranných složek, nejen v případě ovládání vozidel a jejich údržby, ale také např. co se týče využití evakuačních zařízení.

Komunikační a koordinační (IT) systémy

- Bezpečné komunikační systémy a sítě – rádiové sítě, velitelská centra a integrované komunikační platformy pro řešení mimořádných situací.
- Kybernetická bezpečnost a IT infrastruktura pro řízení mimořádných událostí – datová centra, cloudové služby, systémy pro obnovu po havárii a nástroje kybernetické bezpečnosti, které pomáhají chránit kritickou infrastrukturu a zajišťují bezpečnost a řízení IT systémů v nouzových a krizových situacích.

- Obranné a bezpečnostní technologie – zabezpečené komunikační platformy, pokročilé elektronické systémy a řešení internetu věcí pro bezpečnostní a obranné aplikace.
- Řízení dopravy a inteligentní dopravní systémy (ITS) – vývoj inteligentních systémů řízení dopravy, které lze využít jak pro každodenní řízení dopravy, tak v mimořádných nebo krizových situacích.
- Ochrana a monitorování kritické infrastruktury – ochrana a monitorování základní infrastruktury, technologie pro zajištění nepřetržitého provozu a ochrany kritické infrastruktury.
- Odolná IT a technická řešení pro nouzové operace – poskytování odolných IT systémů a technických řešení určených pro náročné podmínky (povětrnostní podmínky, hrubé zacházení, situace s vysokou zátěží apod.).
- Cloudová řešení a řešení datových center pro krizové řízení – cloud computing, ukládání dat a systémy obnovy po havárii, které zajišťují bezpečnost a dostupnost dat v krizových situacích.
- Integrované bezpečnostní systémy pro veřejnou správu – softwarová řešení pro správu dat, koordinaci mezi jednotlivými útvary a zabezpečení komunikačních sítí s cílem zlepšit provozní efektivitu orgánů veřejné správy.

Příklad podniku, který působí v této tematické skupině, přináší Rámeček 8.

Rámeček 8 - URC Systems, spol. s r.o. Zdroj: https://www.urc-systems.cz/

Společnost URC Systems, spol. s r.o. byla založena v roce 1998. Její misí je realizovat řešení náročných požadavků zákazníků v oblastech velení, řízení, informační a komunikační infrastruktury a výkonu činností: (i.) vojskového elektronického průzkumu a sledování, (ii.) ochranného a komunikačního rádiového rušení, (iii.) působení proti bezpilotním systémům a (iv.) bezpečnostních složek při ochraně vlastního území a kritické infrastruktury státu.

Mezi jejich hlavní produkty patří mobilní komunikační a monitorovací centra, která slouží jako mobilní velitelství s vlastními zdroji energie umožňujícími komunikaci a koordinaci zásahů přímo na místě krize. Tato centra jsou vybavena monitorovacími technologiemi, což umožňuje krizovým týmům mít přehled o situaci v reálném čase a rychle reagovat na vznikající potřeby. Stěžejním produktem v této oblasti je mobilní systém JUPITER dodávaný v podobě speciální skříňové nástavby vozidel. Tento systém poskytuje mobilní operační centrum pro řízení zásahů v terénu, komunikační centrum, kamerový dohled, pátrací akce či kontrolní činnost osob a vozidel.

URC Systems se zaměřuje také na ochranu kritické infrastruktury před dronovými hrozbami a nabízí antidronová řešení, jako je JAM-U & GOT-U a přenosné systémy Fast Sky Protection, které dokáží monitorovat, detekovat a rušit drony.

Firma dále vyvíjí robotické systémy, jako např. MVF-5 Tusk, který je určený pro práci v nebezpečných podmínkách, například při likvidaci požárů nebo odstraňování trosek bez ohrožení lidského života.

Dohledové a bezpečnostní systémy

- Elektronické bezpečnostní systémy – vývoj, instalace a správa elektronických bezpečnostních systémů, jako jsou alarmy, CCTV, systémy kontroly přístupu a systémy požární ochrany.
- Dohledové a monitorovací služby – řešení pro dohledové služby, včetně služeb dálkového monitorování nemovitostí, jednotlivců a kritické infrastruktury.

- Služby fyzické bezpečnosti a ochrany – ostraha na místě, služby osobní ochrany, hodnocení rizik a bezpečnostní audity, které zajišťují ochranu soukromých i veřejných prostor před potenciálními hrozbami.
- Inteligentní města a integrovaná bezpečnostní řešení – inteligentní systémy řízení dopravy, veřejného osvětlení a další technologická řešení určená ke zvýšení bezpečnosti ve městech, prevenci kriminality a podpoře reakcí na mimořádné události.
- Výzkum a vývoj v oblasti obrany a bezpečnosti – výzkum, vývoj a aplikace pokročilých technologií zaměřených na zlepšení schopností obranných a donucovacích orgánů.
- Profesní bezpečnostní sdružení a poradenské služby –poradenské a vzdělávací služby, které poskytují poradenství, standardy a osvědčené postupy v oblasti krizového řízení.

Příklady podniků, které působí v této tematické skupině přináší Rámeček 9, Rámeček 10 a Rámeček 11.

Rámeček 9 - JABLOTRON SECURITY a.s. Zdroj: https://www.bezpecnostnicentrum.cz/

Jablotron poskytuje řešení v oblasti zabezpečovacích systémů, která se zaměřují na ochranu majetku a osob. Stěžejním produktem je systém JABLOTRON 100+, profesionální komplexní zabezpečovací systém, který upozorňuje na možné vloupání (otevření dveří, oken, rozbití skleněných výplní, pohyb osob uvnitř objektu), hrozící nebezpečí v podobě požáru (výskyt kouře, zvýšení teploty), záplavy nebo úniku plynu. Je možné jej doplnit o kamerový systém, rozšířit o funkce automatizace a propojit s aplikací MyJABLOTRON, což umožňuje vzdálený přístup a dohled nad bezpečnostními zařízeními v reálném čase. Systém může být napojen na Alarm Receiving Center, který poskytuje nepřetržité monitorování poplachů. V případě aktivace alarmu, například při vloupání nebo narušení bezpečnosti, centrum okamžitě reaguje a vysílá zásahovou jednotku na místo události.

Dále firma poskytuje řešení pro zabezpečení a monitorování vozidel. Systémy pro zabezpečení a monitorování vozidel mohou být také napojeny na Alarm Receiving Center a aplikaci MyJABLOTRON, což umožňuje neustálé monitorování pohybu vozidel a sledování všech jízd včetně ujeté vzdálenosti a spotřeby paliva.

Rámeček 10 - Colsys s.r.o. Zdroj: https://www.colsys.cz/

Společnost Colsys s.r.o. byla založena v roce 1990. Specializuje se na komplexní řešení integrovaných bezpečnostních systémů přizpůsobených potřebám zákazníků v komerčním, veřejném i soukromém sektoru. Mezi hlavní produkty patří systémy elektronického zabezpečení, kamerové systémy (CCTV), požární signalizace (EPS), přístupové systémy a perimetrická ochrana. Dále nabízí automatizaci budov prostřednictvím systémů MaR (měření a regulace) a technická řešení pro energetickou efektivitu budov.

V oblasti bezpečnostních systémů firma dodává poplachové zabezpečovací a tísňové systémy, systémy elektronické kontroly a evidence vstupů, kamerové a videodetekční systémy, systémy perimetrické ochrany a bezpečnostní integrační nadstavby. Aktivity společnosti v oblasti požární bezpečnosti zahrnují elektrickou požární signalizaci, evakuační rozhlas, lokální stabilní hasící systémy, bezdrátový systém požární signalizace či speciální hasící systémy.

Rámeček 11 - Z.L.D. s.r.o. Zdroj: https://www.zld.cz/

Z.L.D. s.r.o. se zaměřuje na integraci technologických řešení pro ochranu obyvatel, infrastruktury, průmyslu a městských oblastí.

Jednou z hlavních technologií, které Z.L.D. nabízí, je platforma iVISEC. Ta slouží pro situace vyžadující okamžitou reakci a správu bezpečnostních hrozeb. iVISEC umožňuje sledování v reálném čase, analýzu videostreamů a používání umělé inteligence pro detekci a analýzu potenciálních rizik. V kombinaci s

technologiemi, jako je Scylla Gun Detection System, iVISEC dokáže identifikovat a upozornit na hrozby, jako je přítomnost zbraní v monitorovaných prostorách.

Společnost Z.L.D. také vyvíjí technologie v oblasti GIS a monitorování pomocí rozsáhlých kamerových systémů. Například v Praze spravuje systém s více než 4 000 kamerami, které poskytují detailní přehled o městské infrastruktuře a zajišťují bezpečnost v reálném čase. Tento systém propojuje GPS jednotky a různé technologie, které podporují jak běžnou bezpečnost, tak zvládání krizových situací v případě ohrožení.

Radarové systémy

- Vývoj radarových systémů pro řízení letového provozu – vývoj a výroba radarových systémů pro řízení a monitorování letového provozu pro civilní i vojenské využití.
- Systémy velení a řízení pro vojenské a civilní použití – komplexní řešení pro řízení a koordinaci vzdušného prostoru, zejména v krizových situacích.
- Poskytovatelé služeb řízení letového provozu – zajištění služeb řízení letového provozu.
- Komunikační systémy pro řízení letového provozu a obranu – vývoj radiokomunikačních a jiných systémů pro řízení letového provozu a obranné operace.

Ochrana kritické infrastruktury

- Řešení pro bezpečnost IT a obnovu po havárii – správa identit, správa IT infrastruktury a obnova po havárii.
- Kritická infrastruktura a záložní energetické systémy – zajištění záložních energetických systémů (generátory a systémy nepřerušovaného napájení), které podporují nepřetržitý provoz kritické infrastruktury, zejména v nouzových situacích.
- Komunikační systémy pro kritickou infrastrukturu a krizové řízení – výroba vysokofrekvenčních rádiových systémů a dalších komunikačních řešení nezbytných pro správu kritické infrastruktury a koordinaci během krizí.
- Telematické systémy pro řízení vozového parku záchranných složek – vývoj a výroba telematických systémů, které zajišťují efektivní trasování, sledování a rozmístění vozidel a prostředků záchranného systému během nouzových operací.

4.3 Vymáhání práva

V oblasti aktivit, technologií a dodávek pro vymáhání práva bylo identifikováno 115 subjektů. Z hlediska svého zaměření a velikosti je tato skupina subjektů velmi různorodá. Nejvíce podniků dosahuje malé velikosti, tedy podniků do 50 zaměstnanců (viz Tabulka 8, která ukazuje podrobnou velikostní strukturu subjektů). Jejich podíl na celkovém počtu subjektů podnikajících v této oblasti dosahuje 56,5 %. Následují střední podniky s 20% podílem na počtu podniků. Nejpočetnějšími velikostními kategoriemi podniků jak v rámci malých a středních podniků, tak také v celém souboru firem jsou podniky s 1 až 5 zaměstnanci (14,78 % z celkového počtu subjektů), 25-49 zaměstnanci (14,78 %) a 55-99 zaměstnanci (13,04 %). Relativně velký podíl prvně uvedené skupiny podniků je však do jisté míry způsoben skutečností, že se jedná o dceřiné společnosti v rámci holdingů, které v oblasti bezpečnosti, resp. prosazování zákona zastupují jiné podniky působící v holdingu.

Tabulka 8 - Počet podniků a objem veřejných zakázek podniků působících v oblasti vymáhání práva podle velikostních kategorií podniků. Zdroj: vlastní zpracování

		Subjekty		Veřejné zakázky	
Kategorie podniku	**Počet zaměstnanců**	**Počet**	**%**	**Objem v Kč**	**%**
	1 - 5	17	14,78	8 992 944	0,28
	6 - 9	9	7,83	37 741 415	1,16
	10 - 19	14	12,17	64 093 307	1,98
	20 - 24	8	6,96	62 193 181	1,92
Malé	25 - 49	17	14,78	302 656 405	9,33
	50 - 99	15	13,04	299 457 852	9,23
	100 - 199	6	5,22	265 626 351	8,19
Střední	200 - 249	2	1,74	0	0,00
	250 - 499	8	6,96	1 791 083 077	55,22
	500 - 999	1	0,87	0	0,00
	1000 - 1499	2	1,74	22 370 544	0,69
Velké	1500 - 1999	2	1,74	388 388 832	11,98
Neuvedeno		14	12,17	704 462	0,02
Celkem		**115**	**100,00**	**3 243 308 371**	**100,00**

Veřejné zakázky v oblasti bezpečnosti získalo 56 subjektů (48,7 % z celkového počtu podniků v této oblasti). Celková hodnota zakázek činila 3,24 mld. Kč. Největší objem zakázek obdržely velké podniky (250 a více zaměstnanců), jak ukazuje Tabulka 8. Tyto podniky získaly 2,2 mld. Kč (67,9 % z objemu zakázek), nejvíce obdržely podniky s 250-499 zaměstnanci, a to 1,79 mld. Kč (55,22 %).

Na základě zaměření dodávaných produktů (výrobků a služeb) je možné subjekty působící v oblasti vymáhání práva či dodávající produkty pro tuto oblast rozdělit do několika specifických tematických skupin:

- Balistická ochrana;
- Forenzní technologie;
- Komunikační technologie;
- Bezpečnostní systémy pro vymáhání práva;
- Technologie pro krizové řízení využitelné pro vymáhání práva;
- IT řešení pro boj proti kyberkriminalitě;
- Logistika a obchod;
- Mediální služby;
- Optické a optoelektronické systémy;
- Radarové systémy;
- Simulace a výcvikové systémy;
- Výroba uniforem, ochranného oblečení a taktického vybavení;
- Vývoj.

Jak vyplývá z Tabulka 9, nejvíce subjektů působí ve skupinách *IT řešení pro boj proti kyberkriminalitě* (21 podniků, tj. 18,26 %), *Technologie pro krizové řízení využitelné pro vymáhání práva* (21 podniků, tj. 18,26 %) a *Bezpečnostní systémy pro vymáhání práva* (17 podniků, tj. 14,78 %). V těchto skupinách podniků byla také alokována většina objemu veřejných zakázek (dohromady 86,13 %). Nejvyšší objem zakázek směřoval do skupiny *Bezpečnostní systémy pro vymáhání práva*, a to 37,21 % z objemu zakázek, do skupiny *IT řešení pro boj proti kyberkriminalitě* 30,26 % a do skupiny *Technologie pro krizové řízení využitelné pro vymáhání práva* 18,65 %. Naopak v oblastech *Optické a optoelektronické systémy* a *Mediální služby* nebyly realizovány žádné veřejné zakázky.

Podniky působící v oblasti vymáhání práva svým zaměřením a aktivitami často přesahují do jiných oblastí bezpečnostních technologií. Jak je zřejmé z Tabulka 9, pouze 32,17 % podniků z oblasti

prosazování zákona současně nepůsobí v jiných oblastech bezpečnosti. Tyto podniky obdržely jen 4,19 % objemu veřejných zakázek, které získaly podniky působící v oblasti vymáhání práva (viz Tabulka 10).

Tabulka 9 - Celkový počet podniků a počet podniků působících pouze v oblasti vymáhání práva podle tematických skupin. Zdroj: vlastní zpracování

Skupina	Subjekty celkem		Subjekty jen v oblasti vymáhání práva		
	Počet	%	Počet	%	Podíl na celkovém počtu subjektů v oblasti vymáhání práva (v %)
Technologie pro krizové řízení využitelné pro vymáhání práva	21	18,26	6	16,22	28,57
IT řešení pro boj proti kyberkriminalitě	21	18,26	0	0,00	0,00
Bezpečnostní systémy pro vymáhání práva	17	14,78	5	13,51	29,41
Komunikační technologie	10	8,70	2	5,41	20,00
Logistika a obchod	9	7,83	5	13,51	55,56
Radarové systémy	7	6,09	2	5,41	28,57
Balistická ochrana	6	5,22	5	13,51	83,33
Simulace a výcvikové systémy	6	5,22	5	13,51	83,33
Forenzní technologie	4	3,48	0	0,00	0,00
Výroba uniforem, ochranného oblečení a taktického vybavení	4	3,48	2	5,41	50,00
Vývoj	4	3,48	0	0,00	0,00
Mediální služby	3	2,61	3	8,11	100,00
Optické a optoelektronické systémy	3	2,61	2	5,41	66,67
Celkem	**115**	**100,00**	**37**	**100,00**	**32,17**

Tabulka 10 - Objem veřejných zakázek v tematických skupinách vymáhání práva. Zdroj: vlastní zpracování

Skupina	Veřejné zakázky celkem		Veřejné zakázky podniků působících jen v oblasti vymáhání práva		
	Kč	%	Kč	%	Podíl na celkovém objemu veřejných zakázek (v %)
Technologie pro krizové řízení využitelné pro vymáhání práva	604 919 691	18,65	57 325 785	42,19	9,48
IT řešení pro boj proti kyberkriminalitě	981 497 164	30,26	0	0,00	0,00
Bezpečnostní systémy pro vymáhání práva	1 206 955 039	37,21	121 000	0,09	0,01
Komunikační technologie	94 712 761	2,92	0	0,00	0,00
Logistika a obchod	59 074 851	1,82	58 904 525	43,35	99,71
Radarové systémy	35 582 077	1,10	16 800 000	12,36	47,21
Balistická ochrana	1 505 824	0,05	1 505 824	1,11	100,00
Simulace a výcvikové systémy	303 139	0,01	303 139	0,22	100,00
Forenzní technologie	17 306 682	0,53	0	0,00	0,00
Výroba uniforem, ochranného oblečení a taktického vybavení	2 901 556	0,09	924 634	0,68	31,87
Vývoj	238 549 587	7,36	0	0,00	0,00
Mediální služby	0	0,00	0	0,00	0,00
Optické a optoelektronické systémy	0	0,00	0	0,00	0,00
Celkem	**3 243 308 371**	**100,00**	**135 884 907**	**100,00**	**4,19**

Níže jsou stručně charakterizovány jednotlivé tematické skupiny podniků.

Technologie pro krizové řízení využitelné pro vymáhání práva

- Technologie pro sledování a řízení dopravy – inteligentní dopravní systémy, systémy detekce vozidel a letecký management.
- Geoprostorová data a mapování – digitální mapy a geoprostorová data a analýzy terénu.
- Drony a navigační technologie – drony, GPS a navigační technologie.
- Bezpečnostní a komunikační systémy – zařízení pro krizovou komunikaci (včetně výstražných a komunikačních systémů pro nouzová vozidla, nemocnice a policii) a technologie pro řízení a koordinaci zásahů v nouzových situacích, jako jsou dispečerské centrály a vysokofrekvenční rádiové systémy.
- Školení a konzultace v oblasti krizového řízení – školení a poradenství zaměřené na bezpečnostní strategie a krizový management.

Příklad podniku, který působí v tomto oboru, přináší Rámeček 12.

Rámeček 12 - Eyedea Recognition s.r.o. Zdroj: https://www.eyedea.cz/cs

Eyedea Recognition vyvíjí technologie pro rozpoznávání objektů v obraze založené na strojovém učení a umělé inteligenci. Společnost založilo v roce 2006 několik výzkumníků jako spin-off firmu ČVUT. Prvním produktem byl software pro rozpoznávání registračních značek automobilů.

Firma poskytuje tyto produkty:

- AI software pro pokročilé rozpoznávání a klasifikaci vozidel (MMR), čtení registračních značek (ANPR) a unikátní technologie pro identifikaci nečitelných registračních značek (Forensic ANPR).
- Software pro detailní klasifikaci vozidel, který rozpoznává kategorii, výrobce, model, generaci, variantu a barvu zachyceného vozidla, a to z předního i zadního pohledu.
- AI software pro čtení registračních značek. Čte jedno i více řádkové RZ včetně rozpoznání státu registrace a ADR tabulky nebezpečného nákladu.
- Software pro vizuální inspekci předních sedadel. Analyzuje obsazenost a počet pasažérů na předních sedadlech, detekuje nedovolené používání mobilního telefonu řidičem, ověřuje použití bezpečnostních pásů.
- Aplikace pro analýzu nekvalitních videozáznamů, která umožňuje rozpoznat lidským okem nečitelné registrační značky.
- Forenzní analýza – sada softwarových nástrojů na bázi AI s pokročilými funkcemi určenými pro forenzní analýzu, které jsou schopny dešifrovat nečitelné registrační značky, sledovat pohyb vozidel a rozpoznávat obličeje. Využitelné jsou zejména pro orgány činné v trestním řízení a forenzní analytiky.
- AI software pro detekci tváří, klasifikaci jejich atributů (věk, pohlaví, emoce atd.) a biometrickou identifikaci osob ve videozáznamech.

IT řešení pro boj proti kyberkriminalitě

- Ochrana sítí a IT infrastruktury – komplexní IT bezpečnostní řešení zaměřená na ochranu sítí, správu IT infrastruktury a zabezpečení proti kybernetickým útokům (penetrační testy, audity kybernetické bezpečnosti a ochrana před kyberzločinem).
- Kybernetické forenzní služby – digitální forenzní analýzy a vyšetřování, včetně analýzy blockchainu, obnovy hesel, sledování počítačového provozu a expertizní činnosti pro orgány činné v trestním řízení.
- Kybernetické vzdělávání a školení – konzultační a vzdělávací služby zaměřené na kyberbezpečnost, včetně školení v oblasti obrany proti kyberútokům, etického hackingu a provozu bezpečnostních operačních center (SOCs).
- Bezpečnostní monitoring a pokročilá technologie – monitorování sítí a zajištění bezpečnosti pomocí pokročilých technologií, včetně hlasové analýzy, biometrie a kryptografických systémů.
- Digitální transformace – digitální transformace podniků s důrazem na bezpečnostní aspekty, což zahrnuje implementaci bezpečnostních řešení v cloudu, správu identit, privilegovaného přístupu a mobilních zařízení.

Bezpečnostní systémy pro vymáhání práva

- Elektronické bezpečnostní systémy – systémy alarmů, sledování (kamerové systémy) a kontroly přístupu.
- Fyzická ochrana a technické služby – fyzická ochrana a vzdálené sledování zahrnující ochranu průmyslových a vojenských objektů, montáž oplocení a dalších fyzických bariér.
- Konzultační a poradenské služby – odborné poradenství v oblasti bezpečnosti.
- Kontrarozvědka a pokročilé technologie – detekce a neutralizace odposlechových zařízení, zabezpečená komunikace a instalace ochranných technologií (např. RF stíněné komory).
- Školení a výcvik – v oblasti speciálních bezpečnostních operací, často s odborníky pocházejícími z ozbrojených složek.

Příklady podniků, které působí v oboru ochrana kritické infrastruktury a bezpečnostní systémy, jsou uvedeny v Rámeček 13 a Rámeček 14.

Rámeček 13 - Trade FIDES. Zdroj: https://www.fides.cz/

Firma Trade FIDES patří mezi přední dodavatele komplexních integrovaných bezpečnostních systémů v České republice. Na trhu bezpečnostních systémů a informačních technologií působí od roku 1995. Je držitelem oprávnění a certifikátů pro činnosti týkající se projektování vývoje, výroby, realizace, servisu a revizí bezpečnostních technologií, jako jsou např. bezpečnostní certifikáty NBÚ či osvědčení mezinárodního řízení jakosti ISO 9001, vydané certifikačním systémem TDS na všechny druhy činnosti, včetně vývoje, výroby, konstrukce a montážních prací až po po-prodejní servis.

Trade FIDES vyrábí více než 100 různých výrobků, které jsou výsledkem vlastního výzkumu a vývoje. Produkuje technologie pro dohledová a poplachová přijímací centra, poplachové zabezpečovací a tísňové systémy, elektronickou kontrolu vstupu, elektrickou požární signalizaci, dohledové videosystémy, grafické nadstavbové systémy, mechanické zábranné systémy, perimetrické detekční systémy, měření a regulace a strukturovanou kabeláž. Využívá bezpečnostní řešení ASSET a LATIS. Systém ASSET je kombinací softwarového a hardwarového řešení, které umožňuje pomocí jediného produktu vyřešit bezpečnost a monitoring budovy nebo areálu, zřizovat přístupy pouze oprávněným osobám, řídit osvětlení, vzduchotechniku a napojení na čidla, sledovat a řídit obsazenost parkovišť apod. Systém LATIS poskytuje služby GNS grafické bezpečnostní nadstavby pro lokální zastřežení, ale také jako dohledové a poplachové přijímací centrum.

Firma dodává integrovaná bezpečnostní řešení pro Armádu ČR a Policii ČR. Dodala např. zabezpečovací systém pro vojenské letiště Náměšť nad Oslavou.

Rámeček 14 - ELTODO, a.s. Zdroj: https://www.eltodo.cz/

Firma Eltodo byla založena v roce 1991, s výrobou vlastních výrobků započala v roce 1996. V současnosti zastřešuje skupinu 10 podniků. Obchodní aktivity skupiny ELTODO jsou orientovány zejména na český a slovenský trh. Podniky celé skupiny dodávají výrobky a řešení pro dopravní systémy, osvětlení, energetiku, TZB, ICT systémy a kamerové systémy.

V oblasti bezpečnosti se firma specializuje na oblasti sdělovací techniky, především na přenosové systémy, systémy pro ochranu osob a majetku, železniční infrastruktury, kamerové systémy včetně pokročilé video analýzy, elektronické zabezpečovací systémy EZS, elektronické požární systémy EPS a automatické samozhášecí systémy ASHS.

Firma disponuje vlastním vývojovým centrem, které působí ve všech oblastech působení koncernu. Je autorem různých patentů, užitných vzorů, průmyslových vzorů a ochranných známek. V rámci výzkumných projektů tradičně spolupracuje s ústavy AV ČR, ČVUT, VŠB-TUA a Žilinskou univerzitou.

Komunikační technologie

- Zabezpečené komunikační systémy – komunikační řešení pro vládní organizace, armádu a bezpečnostní složky (RF technologie, šifrovaná komunikace a systémy pro krizové řízení).
- Komunikační a navigační systémy pro armádu a letectví.
- Systémy pro integrovanou komunikaci a řízení – vývoj a integrace systémů velení a řízení (C2), které zajišťují efektivní komunikaci při krizových operacích.
- Obchod s komunikačními technologiemi.

Příklad podniku, který působí v oboru komunikační technologie, je uveden v Rámeček 15.

Rámeček 15 - ATS-TELCOM PRAHA, a. s. Zdroj: https://www.atstelcom.cz/

Firma ATS-TELCOM PRAHA, a. s. je českou telekomunikační společností zaměřenou zejména na výstavbu a servis komunikačních sítí kritické infrastruktury a kybernetickou bezpečnost. Vznikla v roce 1994.

V oblasti kritické infrastruktury, resp., infrastruktury rozsáhlých sítí navrhuje řešení LAN, MAN, WAN a hybridních hlasových sítí a poskytuje komplexní služby při řešení v oblasti bezdrátových technologií – od mikrovlnných spojů, WiFi sítí až po privátní 5G sítě.

Poskytuje také bezpečnostní poradenství v oboru provozování a správy komunikačních a informačních systémů, včetně vypracování bezpečnostních směrnic a penetračního testování perimetrů.

Další aktivity firmy spočívají ve vývoji a výrobě specifických přepravních boxů určených pro instalaci a provoz ICT, specializovaných dispečerských pracovišť nebo silničních rychloměrů. Dodává také modulární střelnice pro zabezpečení výcviku ve střelbě.

Logistika a obchod

- Obchod – domácí a zahraniční obchod se střelnými zbraněmi, municí, obrněnými vozidly, systémy sledování a dalšími vojenskými a bezpečnostními technologiemi.
- Vojenská logistika a řízení dodavatelského řetězce – optimalizace procesů spojených s dodávkami vojenského a bezpečnostního vybavení a zajištění jeho dostupnosti pro obranné a bezpečnostní složky.
- Doprava nebezpečných materiálů – přeprava vojenských a nebezpečných materiálů.

Radarové systémy

- Systémy řízení letového provozu: Vývoj a výroba radarových systémů pro řízení leteckého provozu, které slouží vojenským i civilním účelům.
- Monitorovací a sledovací technologie – technologie pro sledování letů a dohledové systémy, které jsou využívány při řízení leteckého provozu.
- Radarové systémy pro měření rychlosti a dohled nad dopravou – vývoj radarových zařízení pro měření rychlosti a kontrolu dopravních pravidel.
- Obranné a bezpečnostní radarové systémy – vývoj radarových technologií speciálně zaměřených na obranné a bezpečnostní účely.

Příklad podniku z tohoto oboru ukazuje Rámeček 16.

Rámeček 16 - RAMET s.r.o. Zdroj: https://www.ramet.as/uvodni-strana

Společnost RAMET s.r.o. je českou společností, která vznikla v roce 1992. Zabývá se vývojem, výrobou, servisem a prodejem radarové a anténní techniky pro různé obory, jako jsou radiolokace, silniční rychloměry a elektromechanické inženýrství.

V oblasti bezpečnosti jsou hlavním produktem silniční rychloměry RAMER10, které jsou již pátou generací měřičů rychlosti vyráběných touto společností. Tento rychloměr je dodáván ve dvou variantách – mobilní a stacionární. Je opatřen modulem ANPR, který umožňuje rozpoznat registrační značky vozidel a ověřit data na nich obsažená jejich porovnáním s příslušnou databází. Měření je možno provádět v obou směrech. K dispozici je také GPS systém instalovaný v radaru, který umožňuje jednoznačnou identifikaci místa. Trestné činy jako překročení povolené rychlosti jsou dokumentovány a lze je vidět na displeji ihned po měření.

Balistická ochrana

- Výroba balistické ochrany jedince – neprůstřelné vesty, helmy a štíty.
- Balistické systémy pro letectví – balistické ochranné systémy pro leteckou techniku.
- Balistické materiály a infrastruktura – pancéřové ocelové desky a ochranná betonová zařízení pro vojenské a civilní objekty, které chrání před balistickými a CBRN hrozbami.

Simulace a výcvikové systémy

- Vývoj pokročilého simulačního softwaru – virtuálních prostředí poskytujících realistické tréninkové scénáře pro vojenské a bezpečnostní složky.
- Specializovaný terénní a taktický výcvik.
- Vývoj leteckých simulátorů.
- Simulační technologie pro ozbrojené a bezpečnostní síly – vývoj a implementace výcvikových simulátorů pro různé zbraně a taktické postupy.

Forenzní technologie

- Mobilní forenzní nástroje – vývoj nástrojů pro mobilní forenzní analýzu, které umožňují orgánům činným v trestním řízení extrahovat a analyzovat data z mobilních zařízení.
- Digitální řešení s využitím umělé inteligence (AI) a strojového učení (ML) – vývoj pokročilých digitálních technologií s AI a ML, které pomáhají identifikovat podezřelé osoby nebo podezřelé vzorce chování apod.
- Ochrana proti padělání – vysoce bezpečné hologramy a další technologie, které pomáhají chránit dokumenty a produkty před padělám.

Výroba uniforem, ochranného oblečení a taktického vybavení

- Taktické vybavení pro vojenské a policejní složky – taktické batohy, modulární nosné systémy a další výstroj určené pro speciální jednotky.
- Ochranné vybavení pro záchranné složky – ochranné rukavice a oděvy pro hasiče, vojáky a policii.
- Výroba uniforem pro bezpečnostní složky -: standardizované uniformy pro policii, armádu a záchranné služby.

Vývoj

- Aplikovaný výzkum a vývoj v oblasti obrany a bezpečnosti nezařaditelný do ostatních skupin.

Mediální služby

- Publikační aktivity v oblasti bezpečnosti a obrany.
- Pořádání konferencí, seminářů a dalších akcí v oblasti bezpečnosti a obrany.

Optické a optoelektronické systémy

- Výroba optických a optoelektronických produktů.
- Vývoj přístrojů pro letectví.
- Noční vidění a termovizní zařízení.

4.4 CBRN hrozby

V oblasti CBRN hrozeb dle použitých informačních zdrojů působí 47 subjektů. Nejvíce podniků (22, tj. 47 %) dosahuje malé velikosti, středně velké podniky jsou zastoupeny 30 % (14 podniků) a velké podniky 15 % (7 podniků). Podrobnější členění velikostní struktury přináší Tabulka 11. Z ní jsou zřejmé značné rozdíly v zastoupení firem v jednotlivých velikostních kategoriích. Nejčetnější velikostní kategorií podniků jsou podniky se 100-199 zaměstnanci, kterých je 12 (25,53 %), následují podniky s 25-49 zaměstnanci (7 podniků, 14,89 %) a s 1-5 zaměstnanci (6 podniků, 12,77 %).

Objem veřejných zakázek, které získaly podniky působící v oblasti CBRN hrozeb, dosahoval 906 mil. Kč. Tabulka 11 ukazuje, že 88,8 % objemu veřejných zakázek koncentrují velké firmy, zejména firmy s 500-999 zaměstnanci (558,5 mil. Kč, 61,62 %) a s 250-499 zaměstnanci (246 mil. Kč, 27,15 %).

Tabulka 11 - Počet podniků a objem veřejných zakázek podniků působících v oblasti ochrany před CBRN hrozbami podle velikostních kategorií podniků. Zdroj: vlastní zpracování

		Subjekty		Veřejné zakázky	
Kategorie podniku	**Počet zaměstnanců**	**Počet**	**%**	**Objem v Kč**	**%**
	1 - 5	6	12,77	170 326	0,02
	6 - 9	2	4,26	0	0,00
	10 - 19	5	10,64	481 580	0,05
	20 - 24	2	4,26	1 210 000	0,13
Malé	25 - 49	7	14,89	15 801 434	1,74
	50 - 99	1	2,13	0	0,00
	100 - 199	12	25,53	83 457 817	9,21
Střední	200 - 249	1	2,13	425 996	0,05
	250 - 499	5	10,64	246 135 547	27,15
	500 - 999	1	2,13	558 547 936	61,62
Velké	1000 - 1499	1	2,13	248 050	0,03
Neuvedeno		4	8,51	0	0,00
Celkem		**47**	**100,00**	**906 478 686**	**100,00**

Podniky působící v oblasti CBRN byly dle svého zaměření rozděleny do následujících tematických skupin:

- Stavební materiály a konstrukční prvky;
- Dekontaminace a ochranné prostředky;
- Výzkum a vývoj v oblasti CBRN;
- Filtrační systémy a systémy čištění vzduchu;

- Radiační ochrana a jaderná bezpečnost;
- Ochrana proti výbuchu a balistická ochrana.

Nejvíce podniků (15, tedy 31,91 % podniků z oblasti CBRN) působí ve skupině *Stavební materiály a konstrukční prvky*, jak je patrné z Tabulka 12. Následují skupiny *Dekontaminace a ochranné prostředky* a *Výzkum a vývoj v oblasti CBRN* (v obou skupinách 9 podniků, 19,15 %).

Tabulka 12 - Celkový počet podniků a počet podniků působících pouze v oblasti CBRN ochrany podle tematických skupin. Zdroj: vlastní zpracování

	Subjekty celkem		Subjekty jen v oboru CBRN		
Skupina	**Počet**	**%**	**Počet**	**%**	**Podíl na celkovém počtu subjektů v oblasti CBRN (v %)**
Stavební materiály a konstrukční prvky	15	31,91	4	19,05	26,67
Dekontaminace a ochranné prostředky	9	19,15	7	33,33	77,78
Výzkum a vývoj v oblasti CBRN	9	19,15	2	9,52	22,22
Filtrační systémy a systémy čištění vzduchu	5	10,64	3	14,29	60,00
Radiační ochrana a jaderná bezpečnost	5	10,64	5	23,81	100,00
Ochrana proti výbuchu a balistická ochrana	4	8,51	0	0,00	0,00
Celkem	**47**	**100,00**	**21**	**100,00**	**44,68**

Tabulka 13 ukazuje objem veřejných zakázek získaných podniky působících v oblasti CBRN. Nejvyšší objem veřejných zakázek obdržely podniky z tematické skupiny *Výzkum a vývoj v oblasti CBRN* (796 mil. Kč, tedy 87,82 %). V této skupině se však veřejné zakázky výrazně koncentrovaly jen ve dvou podnicích (první získal 70,16 % objemu veřejných zakázek a druhý 29,8 %).

Tabulka 13 - Objem veřejných zakázek v tematických skupinách CBRN ochrany. Zdroj: vlastní zpracování

	Veřejné zakázky celkem		Veřejné zakázky podniků působících jen v oblasti CBRN		
Skupina	**Kč**	**%**	**Kč**	**%**	**Podíl na celkovém objemu veřejných zakázek (v %)**
Výzkum a vývoj v oblasti CBRN	796 113 852	87,82	558 547 936	85,60	70,16
Dekontaminace a ochranné prostředky	86 993 715	9,60	81 422 802	12,48	93,60
Radiační ochrana a jaderná bezpečnost	12 544 277	1,38	12 544 277	1,92	100,00
Stavební materiály a konstrukční prvky	10 656 516	1,18	0	0,00	0,00
Ochrana proti výbuchu a balistická ochrana	170 326	0,02	0	0,00	0,00
Filtrační systémy a systémy čištění vzduchu	0	0,00	0	0,00	0,00
Celkem	**906 478 686**	**100,00**	**652 515 015**	**100,00**	**71,98**

Níže jsou stručně charakterizovány jednotlivé tematické skupiny podniků.

Stavební materiály a konstrukční prvky

- Řešení pro zajištění ochrany kritické infrastruktury – vývoj a výroba materiálů pro zajištění ochrany kritické infrastruktury, vývoj automatizačních systémů pro zajištění ochrany kritické infrastruktury.
- Stavební a specializovaná ochranná řešení – vývoj a výroba modulárních krytů, výstavba podzemních krytů či vysoce bezpečné infrastruktury, jako jsou protiatomové kryty a panikové místnosti.
- Stavební materiály a konstrukční prvky zajišťující ochranu před CBRN hrozbami – vývoj a výroba speciálních stavebních materiálů a konstrukčních prvků (dveří apod.) s vysokou úrovní ochrany.

Příklad podniku z tohoto oboru ukazuje Rámeček 17.

Rámeček 17 - Tebrix Safety Home s.r.o. Zdroj: https://www.tebrix.cz/

Tebrix Safety Home s.r.o. se zaměřuje na návrh a výstavbu podzemních krytů, jejichž hlavním účelem je ochrana před CBRN hrozbami.

Hlavní oblastí expertizy Tebrix Safety Home je výstavba podzemních protiatomových krytů, které splňují všechny potřebné bezpečnostní požadavky dle ČSN739010 (Navrhování a výstavba staveb civilní ochrany).

Firma zabezpečuje nemocniční a jiné komerční prostory prostřednictvím pancéřových dveří, bezpečnostních kamerových systémů, zabezpečovacích systémů a čidel proti násilnému vniknutí. Dále zajišťuje čistotu vody např. pro vládní budovy (Pražský Hrad, Parlament apod.) pomocí speciálních vodních filtrů, které zajistí konzumní vodu při kontaminaci chemickými či bojovými látkami.

Dekontaminace a ochranné prostředky

- Řešení pro dekontaminaci – specializované systémy pro biologickou, chemickou a radiologickou dekontaminaci, které zajišťují odstranění nebezpečných látek z povrchů, osob a materiálů.
- Ochranné vybavení CBRN – výroba a dodávky ochranných prostředků určených k ochraně osob před hrozbami CBRN (plynové masky, ochrana dýchacích cest, specializované obleky a další osobní ochranné prostředky přizpůsobené nebezpečnému prostředí).
- Skladování nebezpečných materiálů a sanace životního prostředí – správa a skladování nebezpečných materiálů a sanační služby, které čistí a neutralizují nebezpečné látky v životním prostředí.
- Integrovaná řešení ochrany před CBRN hrozbami a krizového řízení – integrovaná řešení, která řeší jak obranu proti CBRN hrozbám, tak i širší problémy krizového řízení (výroba víceúčelového vybavení a logistických systémů).
- Pokročilé materiály a nanotechnologie pro CBRN a lékařskou ochranu – vývoj a využití pokročilých materiálů jako jsou nanovlákna a polymery, které se používají v ochranných prostředcích, zdravotnických filtračních systémech a materiálech zvyšujících ochranu proti CBRN hrozbám.

Příklady podniků z tohoto oboru přinášejí Rámeček 18 a Rámeček 19.

Rámeček 18 - Dekonta CBRN s.r.o. Zdroj: https://www.dekontacbrn.cz/

Dekonta CBRN s.r.o. je dceřinou společností firmy Dekonta a.s. Byla založena v roce 2017. Zaměřuje se na komplexní ochranu před CBRN riziky prostřednictvím prevence a řešení CBRN hrozeb, nakládání s vysoce nebezpečnými látkami, dekontaminace zasažených prostor, vývoje speciálních dekontaminačních zařízení, testování dekontaminačních prostředků, vývoje technologií, produktů a metodik a skladování vysoce rizikových materiálů.

Společnost se podílí na bezpečnostních výzkumných projektech financovaných z národních programů podpory VaV a spolupracuje s vysokými školami univerzitami a různými výzkumnými organizacemi. Příkladem výstupů projektů VaV je zařízení DA-2, což je mobilní dekontaminační jednotka určená k nasazení v těžko přístupných místech, která umožňuje variabilní aplikaci dekontaminačních prostředků, včetně mlhy, pěny nebo oplachu, a je optimalizována pro rychlou a efektivní likvidaci kontaminace v terénu.

Dekonta CBRN poskytuje služby a produkty zaměřené na preventivní ochranu, detekci a eliminaci CBRN hrozeb, a nabízí širokou škálu vybavení pro osobní i kolektivní ochranu, od filtračně-ventilačních systémů až po dekontaminační sady a ochranné masky. K dispozici jsou také specializované detekční soupravy pro rychlou identifikaci chemických látek a detekci výbušnin.

Rámeček 19 - ORITEST spol. s r.o. Zdroj: https://www.oritest.cz/

ORITEST spol. s r.o. byla založena v roce 1992. Společně se svojí dceřinou společností ORIMPEX nabízí produkty a služby zejména v oblastech detekce průmyslových toxických látek a BCHL (bojové chemické látky) a dekontaminace chemických kontaminantů, zejména BCHL.

Společnost disponuje vlastním výzkumným týmem, který je původcem více než 80 patentů, (které jsou v převážné většině využívány při výrobě) a více než 150 vědeckých publikací. Velmi významný je přenos know-how původně zaměřeného zejména na vojenskou oblast do civilního sektoru, především do oblasti ochrany životního prostředí.

Hlavní produkty jsou určeny pro detekci chemických látek, zahrnují detekční trubice, papírky a sady umožňující rychlou identifikaci chemických bojových látek (CWA) a toxických průmyslových látek (TIC). Společnost vyvíjí rovněž detektory s iontově-mobilitní spektrometrií (IMS), což umožňuje přesnou analýzu chemických kontaminantů.

Další oblastí činnosti ORITESTu je vývoj dekontaminačních prostředků, které zahrnují přípravky a zařízení pro odstranění kontaminace z povrchů, osobního vybavení a prostorů. Firma nabízí i výcvikové programy na míru pro CBRN specialisty, zaměřené na praktické dovednosti v detekci a dekontaminaci, první pomoc a osobní ochranu.

Výzkum a vývoj v oblasti CBRN hrozeb

- Simulace a výcvik jako příprava na CBRN hrozby – vývoj pokročilého simulačního softwaru a virtuálních prostředí, které umožní trénovat složité scénáře v realistickém prostředí.
- Jaderné technologie a inženýrství – výzkum v oblasti jaderné energetiky.
- Detekce záření a syntéza materiálů – vývoj syntetických materiálů a detektorů používaných při detekci a měření radiace.
- Elektronické systémy a diagnostické nástroje pro specializovaná prostředí – vývoj elektronických systémů pro automatizaci, robotiku, mechatroniku a diagnostiku životního prostředí, které fungují v extrémních nebo nebezpečných prostředích.
- Integrované obranné, letecké a průzkumné systémy (Intelligence, Surveillance, and Reconnaissance) – vývoj v oblasti obranných technologií, které se prolínají s letectvím, umělou inteligencí.

Příklad podniků z tohoto oboru přináší Rámeček 20.

Rámeček 20 - Vojenský výzkumný ústav, s. p. Zdroj: https://www.vvubrno.cz/

Sekce chemické, biologické a radiační ochrany Vojenského výzkumného ústavu, s. p. (VVÚ) se věnuje výzkumu, vývoji a testování v oblasti chemické, biologické, radiologické a nukleární ochrany. VVÚ se věnuje výzkumu detekčních technologií, ochranných prostředků a dekontaminačních metod v souvislosti s chemickými zbraněmi (CWA), toxickými látkami a radioaktivními materiály.

V oblasti detekce chemických a biologických hrozeb se věnuje vývoji zařízení a metod pro identifikaci CWA, významných toxických chemikálií a biologických agens. Tento výzkum zahrnuje pokročilé metody

vzdálené detekce, integraci detekčních zařízení do monitorovacích systémů a vývoj protokolů pro odběr a analýzu kontaminovaných vzorků.

VVÚ také vyvíjí technologie pro odstranění CBRN kontaminace z terénu, infrastruktury a osobního vybavení. To zahrnuje testování dekontaminačních směsí a metod, které se aplikují jak v laboratorních, tak i polních podmínkách.

Důležitou součástí aktivit VVÚ je testování ochranných a detekčních zařízení, včetně odolnosti materiálů vůči extrémním podmínkám jako je mráz, plameny nebo korozivní látky.

Filtrační systémy a systémy čištění vzduchu

- Ochranné osobní vybavení pro CBRN hrozby – ochranné prostředky, jako jsou plynové masky, filtrační systémy, ochranné oděvy.
- Filtrační systémy pro záchranné prostředky – filtrační systémy pro specializované dopravní prostředky a mobilní vybavení (přístřešky, mobilní úkryty apod.).
- Filtrace z lékařských ?? a nanovláken pro zdravotnictví – pokročilé filtrační technologie založené na využití nanovláken, které jsou využívány pro výrobu lékařských masek a obvazového materiálu.
- Průmyslové filtrační systémy – filtrační systémy pro průmyslové prostředí, které jsou určeny k ochraně pracovníků a zařízení před škodlivinami ve vzduchu.
- Pokročilý vývoj materiálů pro filtraci – vývoj specializovaných filtračních materiálů, například materiálů z nanovláken nebo vyztužené pryže, které nabízejí zvýšenou odolnost a ochranu filtračních výrobků.

Radiační ochrana a jaderná bezpečnost

- Radiační ochrana a monitorovací systémy – vývoj a poskytování systémů pro monitorování a ochranu před ozářením (zařízení pro detekci radiace, radiační bezpečnost v jaderných zařízeních a systémy pro nakládání s radioaktivním odpadem).
- Bezpečnost jaderných elektráren – technologie pro zajištění bezpečného provozu jaderných reaktorů.

Příklad podniků z tohoto oboru uvádí Rámeček 21.

Rámeček 21 - NUVIA a.s. Zdroj: https://www.nuvia.com/cz/

NUVIA a.s. je dceřiná společnost VINCI Construction a divize světového lídra VINCI. Mateřská firma se již více než 60 let zabývá jaderným inženýrstvím a výstavbou nových jaderných zdrojů. Dodává kompletní EPC (Engineering, Procurement, Construction) projekty. Nabízí kompletní odborné služby: vytváření koncepcí, zpracování bezpečnostní zprávy, soulad s předpisy, příprava staveniště, výroba, výstavba, uvádění do provozu, řízení dodavatelského řetězce, elektrická / řídicí instrumentace, vzduchotechnické / ventilační systémy, potrubí, manipulační zařízení, skladovací objekty, speciální prádelna, systémy zpracování odpadů a výpustí.

V oblasti CBRN ochrany aktivity firmy NUVIA spočívají zejména v detekci a měření radiace. Nabízí širokou škálu nejmodernějších a na míru vyrobených detektorů, gama kamer, spektrometrů a dalších nástrojů, které umožňují detekci nebo monitorování v reálném čase, ve venkovním prostředí i uvnitř budov, pomocí přenosných zařízení nebo stacionárních přístrojů.

Firma také dodává řešení pro radiační ochranu a bezpečnost v průmyslu. Poskytuje komplexní služby, které zajišťují, aby podnikové postupy a procesy byly bezpečné a v souladu s příslušnými právními normami a technickými předpisy.

Ochrana proti výbuchu a balistická ochrana

- Balistická ochrana osob a vozidel – vývoj a výroba balistické ochrany osob (balistické vesty, ochranné přilby, pyrotechnické ochranné obleky apod.) a vozidel (systémy balistické ochrany vozidel).
- Řešení pro ochranu infrastruktury – vývoj a výroba materiálů a konstrukčních řešení (např. specializovaných betonů), které zvyšují odolnost vojenské a civilní infrastruktury proti výbuchu a balistickým nárazům.
- Nouzové ochranné systémy – systémy a mobilní a modulární ochranné jednotky (kontejnery), které lze rychle nasadit v nouzových situacích k zajištění balistické ochrany v terénu.
- Systémy pro skladování výbušnin – vývoj a výroba systémů pro skladování a bezpečnou manipulaci s výbušnými materiály.

4.5 Ostatní

Do oblasti Ostatní byly zařazeny podniky, které se specializují spíše na oblast obrany a obranné technologie než na oblast bezpečnosti, ačkoliv jejich technologie, resp. produkty jsou využitelné i v oblasti bezpečnosti, zejména v případě vymáhání práva a ochrany před CBRN hrozbami.

Do oblasti Ostatní bylo zařazeno 37 podniků (tedy 8,6 % z celkového počtu podniků, u nichž byla identifikována vazba k oblasti bezpečnostních technologií). 40,5 % (15 podniků) z nich svým počtem zaměstnanců příslušelo mezi malé podniky a po 9 podnicích patřilo mezi podniky střední velikosti (24,3 %) a velké firmy (24,3 %). Podrobnější členění velikostní struktury přináší Tabulka 14. Z ní je zřejmé, že nejvíce podniků spadá do velikostních kategorií 25-49 zaměstnanců (5, tj. 13,51 %) a dále 50-99 zaměstnanců, 500-999 zaměstnanců a 1-5 zaměstnanců (po 4 firmách).

Tabulka 14 - Počet podniků a objem veřejných zakázek podniků zařazených do oblasti Ostatní podle velikostních kategorií podniků. Zdroj: vlastní zpracování

		Subjekty		Veřejné zakázky	
Kategorie podniku	**Počet zaměstnanců**	**Počet**	**%**	**Objem v Kč**	**%**
	1 - 5	4	10,81	0	0,00
	6 - 9	2	5,41	0	0,00
	10 - 19	2	5,41	0	0,00
	20 - 24	2	5,41	134 781 900	74,49
Malé	25 - 49	5	13,51	0	0,00
	50 - 99	4	10,81	27 704 119	15,31
	100 - 199	3	8,11	747 785	0,41
Střední	200 - 249	2	5,41	283 866	0,16
	250 - 499	1	2,70	466 991	0,26
	500 - 999	4	10,81	3 124 858	1,73
	1000 - 1499	1	2,70	4 704 850	2,60
Velké	1500 - 1999	3	8,11	9 122 250	5,04
Neuvedeno		4	10,81	0	0,00
Celkem		**37**	**100,00**	**180 936 619**	**100,00**

Podniky zařazené do oblasti Ostatní získaly z veřejných zakázek příslušejících oblasti bezpečnosti takřka 181 mil. Kč. Jejich rozdělení dle velikostních kategorií podniků přibližuje Tabulka 14. Objem veřejných zakázek je vysoce koncentrován, 74,49 % jejich objemu získala jediná firma z velikostní kategorie 20-24 zaměstnanců. 51,4 % podniků nezískalo žádnou veřejnou zakázku.

Na základě svého zaměření byly podniky z oblasti Ostatní rozděleny do tří specifických skupin:

- Letecká technika;
- Obrněná vozidla;
- Střelné zbraně.

Počet podniků v těchto skupinách a objem veřejných zakázek ukazuje Tabulka 15. Nejvíce podniků (15, tj. 40,5 % z počtu podniků v oblasti ostatní) se specializuje na obor střelných zbraní. Ve zbývajících skupinách – Letecké technice a Obrněných vozidlech působí po 11 podnicích. Zastoupení podniku s nejvyšším objemem veřejných zakázek ve skupině Obrněná vozidla způsobilo, že tato skupina co do objemu veřejných zakázek výrazně vyniká nad skupinami ostatními.

Tabulka 15 - Počet podniků a objem veřejných zakázek podniků působících v oblasti Ostatní podle tematických skupin. Zdroj: vlastní zpracování

	Subjekty		Veřejné zakázky	
Skupina	**Počet**	**%**	**Objem v Kč**	**%**
Letecká technika	11	29,7	29 440 219	16,3
Obrněná vozidla	11	29,7	136 843 284	75,6
Střelné zbraně	15	40,5	14 653 117	8,1
Celkem	**37**	**100,0**	**180 936 619**	**100,0**

Níže jsou stručně charakterizovány jednotlivé tematické skupiny podniků.

Střelné zbraně

- Výroba střelných zbraní – vývoj a výroba střelných zbraní – pistolí, pušek a samopalů.
- Výroba střeliva a výbušnin – výroba munice a výbušnin pro vojenské, policejní a civilní účely.
- Distribuce a velkoobchod se střelnými zbraněmi a střelivem – obchod a dodávky střelných zbraní, střeliva a vojenského vybavení.
- Likvidace střeliva, střelných zbraní a pyrotechnické služby – specializované služby související s likvidací a ničením střelných zbraní, střeliva a výbušnin.

Příkladem podniku z tohoto oboru je Česká zbrojovka a.s., bližší informace uvádí Rámeček 22.

Rámeček 22 - Česká zbrojovka a.s. Zdroj: https://www.czub.cz/

Česká zbrojovka a.s. je jedním z nejvýznamnějších výrobců ručních palných zbraní na světě. Od roku 2020 je součástí mezinárodního holdingu Colt CZ Group. Společnost má rozsáhlou distribuční síť zahrnující více než 100 zemí a zaměstnává více než 1 300 lidí.

Zaměřuje se na výrobu vysoce kvalitních zbraní, které nacházejí uplatnění v armádách, policejních sborech i mezi sportovními střelci a lovci. Mezi klíčové produkty patří samopaly CZ SCORPION EVO 3, útočné pušky CZ BREN 2 a řada pistolí CZ P-10. Tyto zbraně jsou ve výzbroji českých i zahraničních bezpečnostních složek.

V oblasti bezpečnostních technologií firma podporuje inovace, včetně aplikace moderních materiálů a technologií pro zvýšení efektivity a bezpečnosti svých produktů. Například modely CZ BREN 2 a CZ

SCORPION EVO 3 jsou založeny na modulární koncepci, která umožňuje přizpůsobení zbraní různým taktickým scénářům a využití speciálních optických systémů.

Letecká technika

- Výroba letadel – konstrukce a výroba letadel a vrtulníků.
- Servis a modernizace letecké techniky – údržba, opravy a modernizace vojenských letadel včetně vrtulníků.
- Avionika a integrace systémů – integrace a modernizaci avionických systémů.
- Výroba leteckých komponentů – výroba vysoce přesných komponentů využívaných v letecké technice.

Příklad podniku z tohoto oboru přináší Rámeček 23.

Rámeček 23 - Česká letecká servisní a.s. Zdroj: https://www.ceslet.cz/

Česká letecká servisní a.s. (CLS) je součástí holdingu Czechoslovak Group. Zaměřuje se na integraci avionických systémů a instalaci speciálního vybavení do letadel a vrtulníků, a to jak pro civilní, tak vojenský sektor.

Klíčové aktivity v oblasti bezpečnostních technologií zahrnují modernizaci vojenských letadel a vrtulníků, instalaci pokročilých radionavigačních a komunikačních systémů. CLS je certifikována podle evropských standardů PART 145 a PART 21, což jí umožňuje poskytovat komplexní řešení zahrnující návrh technických modernizací, instalaci, certifikaci a následné školení uživatelů.

V oblasti vojenských a bezpečnostních projektů má společnost oprávnění k výrobě a údržbě vojenské letecké techniky. Instalované systémy často zahrnují zařízení od renomovaných výrobců, mezi něž patří Honeywell, FLIR, Garmin či L3Harris. Tyto technologie zahrnují například pokročilé senzory, komunikační moduly a radarové systémy, které zlepšují schopnosti detekce a reakce na bezpečnostní hrozby.

CLS rovněž poskytuje servis avioniky a řešení pro civilní letecký sektor, což zahrnuje modernizaci avionických systémů a implementaci bezpečnostních technologií i na komerčních a soukromých letadlech. Společnost je schopná realizovat projekty na více než 12 platformách v 15 zemích světa.

Obrněná vozidla

- Konstrukce a výroba obrněných vozidel – konstrukce, vývoj a výroba obrněných vozidel pro vojenské a policejní využití.
- Dodávky těžkých vojenských nákladních vozidel – dodávky těžkých nákladních vozidel a specializovaných vojenských nákladních vozidel.
- Úpravy a opravy vozidel pro vojenské použití – úpravy a opravy stávajících vozidel pro vojenské využití.

Příklad podniku z tohoto oboru ukazuje Rámeček 24.

Rámeček 24 - DAJBYCH plus s.r.o. Zdroj: https://www.dajbych.cz/

DAJBYCH plus s.r.o. se věnuje prodeji, úpravám a servisu terénních a speciálních vozidel pro ozbrojené a záchranné složky.

Jednou z hlavních oblastí aktivit firmy je dodávka a přizpůsobení terénních vozidel pro specifické potřeby dle potřeb zákazníka. Mezi nejčastěji modifikovaná vozidla patří modely Toyota Hilux, Land Cruiser a Land Rover Defender, které jsou upravovány pro použití v armádě, policii a při záchranných operacích. Vozidla jsou vybavována technologiemi pro zvýšení odolnosti, pohyblivosti a bezpečnosti, včetně balistické ochrany, komunikačních nebo senzorových systémů.

5 Závěry

Cílem této studie bylo charakterizovat trh bezpečnostních technologií v ČR, zejména identifikovat nabídku technologií a řešení v jednotlivých oblastech bezpečnosti – kybernetické kriminalitě, krizovém řízení, vymáhání práva a CBRN hrozbách – a dále identifikovat specifické tematické skupiny v těchto oblastech a jejich rozsah.

Primárním účelem bylo vyzkoušet přístupy a informační zdroje k průzkumu trhu bezpečnostních technologií. Hlavní poznatky v oblasti přístupu a informačních zdrojů je možné shrnout následovně:

- Neexistuje žádná centrální (úplná) databáze, která by obsahovala seznamy podniků operujících na poli bezpečnostních a obranných technologií a jejich stručnou charakteristiku. Pro analýzy trhu bezpečnostních a obranných technologií je nezbytné kombinovat různé informační zdroje přinášející seznamy podniků.
- Veřejně dostupné informace o ekonomických výsledcích podniků jsou dostupné jen pro minoritní část firem. To významně omezuje hodnocení poptávky po bezpečnostních a obranných technologiích, zejména v případě mezipodnikové poptávky.
- Registr smluv neobsahuje informace o veřejných zakázkách s utajovaným obsahem. To může významně omezovat hodnocení poptávky veřejného sektoru po bezpečnostních a obranných technologiích.
- Veřejně dostupné informace o podnicích prezentované na jejich webových stránkách často přinášejí spíše marketingové informace než informace o technologických řešeních a technologické vyspělosti podniků.

Ve světle těchto metodických omezení je třeba chápat závěry provedené analýzy trhu bezpečnostních a obranných technologií.

Vypracování přehledu o tomto trhu bylo druhým účelem předložené studie. Provedená analýza ukázala, že šíře produktů a aktivit sledovaných firem významně přesahuje vymezení jednotlivých oblastí bezpečnostního trhu. Příčinou může být, že podniky se při rozvoji svých aktivit neřídí vymezením jednotlivých oblastí, ale spíše poptávkou po bezpečnostních technologiích. Polovina podniků tedy působí ve více než jedné oblasti, nejčetnější je kombinace oblastí vymáhání práva a krizového řízení (pětina podniků). Následuje oblast kybernetické bezpečnosti a kombinace oblastí kybernetické bezpečnosti, vymáhání práva a krizového řízení.

Analýza strany nabídky identifikovala v jednotlivých oblastech bezpečnostního trhu specifické segmenty, resp. tematické skupiny a ukázala šíři produktů, které poskytují podniky působící v těchto tematických skupinách. V oblasti kybernetické bezpečnosti nejvíce podniků působí v tematické skupině *Prevence kyberkriminality a řešení kybernetické bezpečnosti.* Firmy podnikající v oblasti krizového řízení se zaměřovaly zejména na nouzové a záchranné vybavení (42 % podniků). V oblasti vymáhání práva aktivity řady podniků přesahují do jiných oblastí, proto téměř pětina podniků působí ve skupině *Technologie pro krizové řízení využitelné pro vymáhání práva* a stejný počet ve skupině *IT řešení pro boj proti kyberkriminalitě*. Téměř třetina podniků z oblasti CBRN hrozeb se věnuje problematice stavebních materiálů a konstrukčních prvků a pětina dekontaminaci a ochranným prostředkům. Ve zbývající oblasti zahrnující leteckou techniku, obrněná vozidla a střelné zbraně nejvíce podniků (41 %) působilo ve skupině střelných zbraní.

Vzhledem k nedostupnosti dat pro hodnocení celkové poptávky a poptávky v podnikovém sektoru byla strana poptávky analyzována jen v případě veřejného sektoru. Jako indikátor poptávky veřejného sektoru po bezpečnostních technologiích byl využit objem veřejných zakázek realizovaných v oblasti bezpečnosti. Analýza ukázala, že tento objem je vysoce koncentrován jak na úrovni oblastí, tak také na úrovni jednotlivých firem. Téměř dvě pětiny směřovaly do oblasti kybernetické bezpečnosti. Celkově polovinu objemu veřejných zakázek získalo pouhých 5 podniků (tj. 1,16 %), přičemž 10 podniků obdrželo více než dvě třetiny objemu zakázek.

Na úrovni identifikovaných tematických skupin v oblasti kybernetické bezpečnosti nejvíce veřejných zakázek směřovalo do skupiny *Digitální transformace a IT poradenství*. V oblasti krizového řízení nejvyšší objem veřejných zakázek byl alokován ve skupině *Komunikační a koordinační (IT) systémy*. V oblasti vymáhání práva více než třetinu objemu veřejných zakázek získaly podniky z tematické skupiny *Bezpečnostní systémy pro vymáhání práva*. V oblasti CBRN hrozeb veřejné zakázky plynuly zvláště na výzkum a vývoj v oblasti CBRN hrozeb. Ve zbývající oblasti nejvyšší objem veřejných zakázek směřoval do firem, které se věnují výrobě, dodávkám a servisu obrněných vozidel.

6 Odkazy a datové zdroje

[1] European Commission (2022): EU Civil Security Stakeholder catalogue. Dostupné na: *https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-stakeholder-catalogue_en*

[2] Informační systém výzkumu, vývoje a inovací. Dostupné na: *https://www.isvavai.cz/*

[3] Asociace obranného a bezpečnostního průmyslu České republiky: seznam členů. Dostupné na: *https://aobp.cz/clenove/*

[4] Czech Digital Solutions: katalog společností. Dostupné na: *https://czechdigitalsolutions.cz/cs/organizace/?categories=70861f98-6f0c-409a-8e30-3bcd5fb6206e*

[5] SystemOnLine: Přehled dodavatelů řešení informační bezpečnosti. Dostupné na: *https://www.systemonline.cz/dodavatele-it-sluzeb-a-reseni/informacni-bezpecnost/*

[6] IDET 2023, seznam vystavovatelů. Dostupné na: *https://www.ibvv.cz/cs/akce/idet-23065/vystavovatele*

[7] PYROS – ISET 2023, seznam vystavovatelů. Dostupné na: *https://ikatalog.bvv.cz/pyros-iset/_fexc9988&nom=0*