Moderní zbraňové systémy jsou vlastně obrovské propojené počítače vybavené množstvím senzorů. Letadla, rakety, drony, ale i tanky a pěchota mezi sebou neustále komunikují a vytvářejí tak digitální bojiště.

Každým rokem se tato situace posouvá dál s tím, jak pokračuje technologcký rozvoj a miniaturizace. Zřejmě nejdále je v této oblasti projekt bojového letadla Lockeed Martin F-35 Lightening II. Vize generálů je jasná, data jsou neustále sdílena, aktualizována podle vývoje na bojišti a díky informační nadvládě lépe informovaná strana porazí zaostalejšího protivníka. Samozřejmě je nutná schopnost data vyhodnocovat a volit na jejich základě vhodné postupy.

K napsání pár řádek na toto téma mě navedl článek o vypínání tanků na dálku (zde).

Hned na začátku si musíme říci, že jsou situace, kdy digitální bojiště nemá očekávané benefity. Potřebujete mít aspoň trochu sofistikovaného protivníka. Proč tento paradox? Protože přes absolutní převahu digitálního boijiště nedokázaly USA, tedy tahoun této strategie, zvítězit v Afghanistánu. Proti "středověkému" bojovníkovi s kalašnikovem, kterého nerozeznáte od pasáčka koz, kterým i nejspíš zároveň je, a kterého vybombardováním nemůžete poslat do zmíněného středověku, protože už tam fakticky je, tam vám digitální převaha nepomůže.

Největší míru informační výměny dnes zaznamenáme v oblasti satelitů - letadel (ať již AWACS, bojových, dronů,...), radarů, protivzdušné obrany, lodí a raket. Datalinky mezi tím vším a výměna dat funguje v reálném čase a při správném použití to může být velmi efektivní řešení jak pro obranné, tak útočné operace.

Nebudeme ale nyní rozebírat výhody, podívejme se na rizika, která stojí za to zvážit, než se každý stát do tohoto konceptu zapojí.

Možnosti ovlivnění

Zbraně jsou vlastně počítače. Počítač pohání a obsluhuje software. Každé čidlo, od radaru, přes různá měření otáček, tlaku,..., rádio,... to vše přijímá nějaké údaje a ty většinou digitalizuje. Digitální data krmí sotware, který se na základě algoritmů buď přímo rozhoduje, nebo poskytuje informace obsluze, která pak na základě toho činí rozhodnutí.

Z toho vyplývají okruhy problémů, které mohou nastat buď samostatně, nebo v kombinaci:

- ovlivnění přímo rozhodování software s dopadem do funkčnosti zbraně jako celku, nebo části

- ovlivnění obsluhy a její schopnosti se správně rozhodnout
- design řešení přímo předpokládá, že musí umožnit nějakou formu ovládnutí

- sdílení dat protivníkovi, který je následně může použít pro své rozhodování a protiakce

Software

Software je dílo programátorů, vlastně miliony řádek zdrojového kódu; desítky a stovky rozhranní mezi různými systémy, kde se data předávají a transformují.

Pro zajímavost link na počet řádek zdrojového kódu v různých projektech: https://informationisbeautiful.net/visualizations/million-lines-of-code/
.

Samotný software ve zbrani má nějakou míru bezpečnosti a hacknutelnosti. Stejně jako váš telefon, nebo počítač. To samé komunikační či ovládací linka v rámci bojiště.

Navíc si nekupujete se zbraní od výrobce zdrojový kód obslužného software zbraně, ale zkompilovanou verzi. A pokud se ke zdrojovému kódu dostanete, není snadné v něm "trojského koně" nebo zadní vrátka najít. Mít zdrojový kód totiž vůbec neznamená mu také rozumět a chápat miliony řádků kódu je opravdu na velký tým a hodně času. To stojí

astronomické peníze.

Běžným standardem států je, že pro vlastní armádu se zbraně vyrábějí lepší, či méně omezené a exportní zbraně obsahují různá omezení. To platí odjakživa, ale možná se to změní s nástupem korporací, které mnohdy již nyní mají větší moc než vlády menších států.

Z toho vyplývá klíčové riziko - náchylnost na úplné vyřazení zbraně, nebo zhoršení klíčových parametrů externím zásahem do obslužného software.

Zdrojem omezení funkčnosti zbraňového systému mohou například být:

1. dálkové vypnutí zbraně protivníkem. Velmi snadné, pokud nakoupíte například protiletadlové rakety, které neumožní navedení na letadlo země výrobce. Tuto funkci nemusí ani v případě stávajícího konfliktu žádná strana využít. Nehraje se s tak velkými kartami, aby stálo za to na tuto funkčnost upozornit. Navíc by to mohlo kazit prodejní kšefty. Neumím posoudit, zda je možné dálkově vypnout, či zhoršit výkonové parametry např. tanků Leopard v Turecku, jak je uvedeno ve článku výše, ale drobným softwarovým zásahem se dá dramaticky ovlivnit třeba životnost komponent, přesnost,... Jako vstupní bod signálu může působit každé čidlo, kterému je zaslána daná sekvence vstupů. Tato funkčnost může být aktivní (dodavatel zbraně aktivně spustí chování) a nebo pasivní - raketa na dané GPS souřadnice nikdy nepřiletí. Vůbec ověření existence těchto funkčností je problém.

2. jakýkoli mechanismus obnovování licenčních klíčů. Nepřijde nový licenční klíč? Máte ze zbraně hromadu šrotu. Nemáte všechny licenční klíče? Nemůžete využít celou funkčnost.

3. hacknutí zbraně během bojové činnosti - tato možnost teprve nabude na významu s rozvojem autonomních zbraní a dronů. Převzetí kontroly nad útočícími drony se dle tisku povedlo Rusům v Syrii.

4. zmatení řídícího software ˇat již zahlcením dat, nebo falešnými daty

5. hacknutí zbraně při běžné kontrole či údržbě (tj. fyzická přítomnost) - nová verze obslužného software má patřičné úpravy. Mnohdy se ale stačí zaměřit na drobnosti, které ovlivňují výkon a životnost a nemusí mít nic společného se softwarem.

6. vymysleli bychom i další, třeba harwarové díry skryté v návrhu zbraně, které podporují

žádoucí chování.

Obecně jsou dále elektronické součástky citlivé i na elektromagnetický pulz. Špatně chráněný obvod může shořet. Mimochodem proto bývalý Sovětský svaz preferoval elektronky.

Jaké z výše uvedeného učinit závěry? Dle mého minimálně tyto:

1. Každý stát by měl udržovat určité zastoupení "hloupých" zbraní. Tyto zbraně fungují za každých podmínek, nelze je hacknout a fungují jako hrubá síla, když vše selže.
2. Jakýkoli nákup sofistikovaného zbraňového prostředku ze zahraničí, či danému státu neloyální firmy znamená vysoké riziko, že zbraň nebude v případě konfliktu použitelná, nebo dostatečně funkční pro dané použití. Proto by státy měly využívat vlastních výzkumných a vývojových kapacit.

3. Pokud by všichni nakupovali zbraně od pár dodavatelů (současný stav), je možné, že se dočkáme doby, kdy dodavatel, či jeho stát, ovládne všechny státy, kam dodali zbraně díky tomu, že ty zbraně budou kontrolovat.
4. je velké riziko, že samoučící se zbraně (vysoká míra učení se a autonomie) se zvrtnou jednoduše proto, že není možné vše hardwarově a softwarově ošetřit a otestovat. Každý software má chyby, s tím jsme se naučili žít, ale ve chvíli, kdy software bude sám rozhodovat o životě a smrti, je to velký problém a sestup do nekončící spirály.

Pokud si myslíte, že se to týká jenom zbraní, zamyslete se nad internetem věcí a možností dálkově ovládat domácí spotřebiče, nebo elektrárnu, vodárnu, či nemocnici...

{jcomments on}