fundacja instytut

CYBERBEZPIECZEŃSTWA

Jak działają szpiedzy?

fundacja instytut
CYBERBEZPIECZEŃSTWA

Wiktor Sędkowski

Badacz zabezpieczeń
Tester penetracyjny

Witold Pizło

Były oficer jednej ze służb specjalnych.

Obecnie prowadzi działalność akademicką oraz szkoleniową z zakresu:
- prewencji kontrwywiadowczej dla biznesu,
- wojny informacyjnej,
- cyberbezpieczeństwa,
- szkoleń antyterrorystycznych.

Witold Pizło

Były oficer jednej ze służb specjalnych.

Prowadzi również profil edukacyjny „Black Prism” na platformie FB, dotyczący tematyki służb specjalnych, przeciwdziałania zagrożeniom wywiadowczym oraz dywersji psychologicznej.

AGENDA

- **SZPIEDZY**
- CYBEROPERACJE
- POSTAWA OBYWATELSKA

Szpieg

- Zadaniem szpiegów jest odkryć tajemnice innych –krajów, firm, osób
- Najlepiej tak, aby szpiegowani nie zorientowali się, że tajemnice zostały im wykradzione.
- Starają się utrzymać w tajemnicy charakter swojej misji – podają się za inne osoby, komunikują z mocodawcą w ukryty sposób itd.
- Zwalczaniem szpiegostwa i rozpoznawaniem go zajmuje się kontrwywiad np. Agencja Bezpieczeństwa Wewnętrznego.

Szpieg

- Funkcjonariusze organizacji wywiadowczej (etatowi oficerowie wywiadu)
  - cywilnego
  - wojskowego

- Nielegałowie
- Szpiedzy uśpieni
- Agenci
- Tajni współpracownicy

Stanisław Hoc
Uniwersytet Opolski
ORCID: 0000-0003-4248-3664

Wymiana agentów wywiadu – aspekty prawne i polityczne

Przyjmuje się, że agent jest najwyższej kategorii i najbardziej wykwalifikowanym osobowym źródłem informacji służby specjalnej, głównie wywiadowczej, niebędącym jej kadrowym pracownikiem. Agent może działać prowadzony bezpośrednio przez centralę, oficera rezydentury legalnej lub nielegalnej bądź pośrednika. Grupa agentów działająca dla tej samej służby i realizująca wzajemnie uzupełniające się zadania zwana jest siatką agenturalną lub wywiadowczą[1].

Często w publikacjach terminem „agent" określa się kadrowych pracowników służb specjalnych, co nie jest zgodne z terminologią używaną w wielu służbach. Dla rozważań zawartych w artykule przyjmuję termin „agent", obejmując nim zarówno agentów *sensu stricto* jak i pracowników (funkcjonariuszy) służb specjalnych, realizujących zadania wywiadowcze, niekorzystających z „przykrycia" dyplomatycznego. „Przykrycie" to oficjalna pozycja społeczna i zawodowa agenta lub oficera wywiadu, także nielegalnego, pozorująca wobec otoczenia normalną i wiarygodną egzystencję.

Szpiedzy

Szpiegostwo

- Szpiegostwo cybernetyczne to działanie polegające na wykorzystaniu środków cyfrowych w celu uzyskania nielegalnego dostępu do tajnych informacji, zwykle w celu uzyskania korzyści politycznych, wojskowych lub handlowych.
- W przeciwieństwie do tradycyjnego szpiegostwa, które obejmuje fizyczną infiltrację, cyberszpiegostwo odbywa się w środowisku cyfrowym, dzięki czemu jest trudniejsze do wykrycia i łatwiejsze do przeprowadzenia z odległych obszarów.
- Rządy, korporacje, a nawet osoby prywatne mogą paść ofiarą tych ataków, w których celem są cenne dane, takie jak tajemnice handlowe, własność intelektualna lub tajemnice państwowe.

Pablo Gonzalez

Szpiegostwo

- Paweł Rubcow, agent wywiadu wojskowego GRU.
- Zatrzymany przez Polskę na granicy polsko-ukraińskiej 27 lutego 2022 r.
- Podawał się za dziennikarza hiszpańskiego i używał hiszpańskiego nazwiska Pablo Gonzales.
- Ur. 1982 w Moskwie
- W 1991 r. wyjeżdża z Matką do Hiszpanii. Zmienia imie, zachowy paszporty: hiszpański i rosyjski. Kończy slawistykę, zaczyna zajmować się dziennikarstwem
- Zbierał informacje na Ukrainie dla rosyjskich służb specjalnych. Celem było też dobycie zaufania opozycjonistów rosyjskich.
- Po zatrzymaniu na znalezionych u niego nośnikach danych zidentyfikowano szczegółowe raporty o działaniach Żanny Niemcowej i osób z jej otoczenia.
- Interesował się w szczególności uczestnikami letniej szkoły dziennikarstwa z Ukrainy i Stanów Zjednoczonych.

Pablo Gonzalez

https://www.agents.media/the-russian-who-was-following-zhanna-nemtsova-travelled-together-with-a-russian-mili

агентство

Поддержать

The Russian who was following Zhanna Nemtsova travelled together with a Russian military intelligence officer

30 ноября 2023

Spanish journalist Pablo Gonzalez (Pavel Rubtsov according to his Russian passport), who was detained in Poland in February 2022 on charges of working for the Russian Main Intelligence Directorate (GRU, country's military intelligence), took the same flights as intelligence officer Sergei Turbin, Agentstvo revealed. This may confirm the accusation made by the Polish intelligence services.

Details. The connection between Gonzalez-Rubtsov and Turbin is evidenced by data from the hacked Sirena-Travel flight-booking database (it was breached by hackers from the Ukrainian Muppets group in September 2023). Among the leaked data, Agentstvo found evidence that on June 16, 2017, tickets to S7 airline flights from Moscow to St. Petersburg and back were purchased using the passport details of Rubtsov and Turbin. The tickets were purchased together at the office of the Orbita-N company at Paveletsky railway station in Moscow.

- **Why is Turbin an intelligence officer?** According to leaked Russian government databases, Turbin, born in 1968, as well as his wife and son, regularly listed 50 Narodnogo Opolcheniya St.as their place of residence in Moscow. This was the address Turbin listed when registering his car, and it also appeared on tickets the man received in 2006, 2008 and 2009. In 2019, Turbin listed the same address when signing a contract for internet services with Corbina telecom provider (this leak is publicly available).

Żanna Niemcowa

Forum Krynica

Szpiegostwo

„Czasem komuś brakowało prądu w komórce czy w laptopie. Nie mówiąc o pracy na wyjeździe, tam zawsze dużo się działo, latały ładowarki, powerbanki. Teraz się zastanawiam, czy on mógł zasysać od nas jakieś dane, kogoś rozpracowywać”

Rosyjska siatka szpiegowska

- Grudzień 2023: Sąd Okręgowy w Lublinie skazał 14 z 16 oskarżonych cudzoziemców za udział w przygotowywaniu akcji dywersyjnych i sabotażowych na terenie Polski
- Zajmowali się m.in. rozpoznawaniem infrastruktury krytycznej, w tym obiektów militarnych i portów morskich
- Obserwowali port Lotniczy w Jasionce, dworzec kolejowy w Rzeszowie, montowali kamery.
- Planowali wysadzenie pociągów, a nawet zabójstwa
- Ogłaszając wyroki skazujące trzem oskarżonym na najniższe kary sąd uchylił areszt tymczasowy
- Yaroslav B. zartrzymany końcem października

Rosyjska siatka szpiegowska

Polskie służby zatrzymały obywatela Rosji, który miał działać na terenie Polski i współpracować z obcym wywiadem. Według informacji Polskiej Agencji Prasowej, miał on realizować zadania polegające m.in. na rozpoznawaniu infrastruktury krytycznej w kilku województwach.

Polska Agencja Prasowa (PAP) podaje, że Agencja Bezpieczeństwa Wewnętrznego (ABW) zatrzymała kolejną osobę, która na terenie Polski miała brać udział w działaniach siatki szpiegowskiej pracującej na rzecz Rosji.

– Rosyjscy szpiedzy wpadają jeden po drugim! Kolejny sukces śledczych Prokuratury Krajowej i ABW. Schwytano szpiega, który działał pod płaszczykiem sportowca. Rosjanin był zawodnikiem 1-ligowego klubu. To już 14 zatrzymany członek rozpracowanej przez nas siatki szpiegowskiej. Dziękuję prokuratorom i funkcjonariuszom ABW za zaangażowanie w obronie Ojczyzny! — poinformował Zbigniew Ziobro na Twitterze.

BBC

Home News US Election Sport Business Innovation Culture Arts Travel Earth Video Live

Firm hacked after accidentally hiring North Korean cyber criminal

16 October 2024

Share Save

Joe Tidy
Cyber Correspondent, BBC World Service

Getty Images

A company has been hacked after accidentally hiring a North Korean cyber criminal as a remote IT worker.

The unidentified firm hired the technician after he faked his employment history and personal details.

Once given access to the company's computer network, the hacker downloaded sensitive company data and sent a ransom demand.

The firm which is based in the UK, US or Australia did not want to be named.

Szpiegostwo

- Szpiedzy często wykorzystują **wiadomości phishingowe**, aby nakłonić ludzi do ujawnienia krytycznych informacji lub umożliwienia dostępu do systemów wewnętrznych. E-maile te mogą wydawać się autentyczne, często kopiując wiarygodne źródła, ale zawierają szkodliwe linki lub załączniki.

- **Złośliwe oprogramowanie**, takie jak trojany, programy szpiegujące lub ransomware, jest często instalowane w systemach docelowych podczas operacji cyberszpiegowskich. Po dostaniu się do środka złośliwe aplikacje mogą monitorować aktywność, zbierać naciśnięcia klawiszy i kraść ważne informacje.

- Cyberszpiedzy często szukają **luk w oprogramowaniu lub systemach**, które nie zostały załatane. Luki te stanowią tylne wejście dla hakerów, umożliwiając im penetrację sieci i pobieranie poufnych informacji.

- **Inżynieria społeczna - manipulowanie ludźmi w celu uzyskania poufnych informacji. Cyberszpiedzy mogą podszywać się pod zaufane osoby lub podmioty, aby nakłonić pracowników do zapewnienia dostępu do zastrzeżonych obszarów sieci.**

- Zaawansowane trwałe zagrożenia (APT) - długotrwałe i ukierunkowane cyberataki, w których intruz uzyskuje dostęp do sieci i pozostaje niewykryty przez długi czas. Celem jest ciągłe pozyskiwanie cennych informacji bez uruchamiania alarmów lub bycia wykrytym.

Szpiegostwo

- Szpiedzy często wykorzystują **wiadomości phishingowe**, aby nakłonić ludzi do ujawnienia krytycznych informacji lub umożliwienia dostępu do systemów wewnętrznych. E-maile te mogą wydawać się autentyczne, często kopiując wiarygodne źródła, ale zawierają szkodliwe linki lub załączniki.

- **Złośliwe oprogramowanie**, takie jak trojany, programy szpiegujące lub ransomware, jest często instalowane w systemach docelowych podczas operacji cyberszpiegowskich. Po dostaniu się do środka złośliwe aplikacje mogą monitorować aktywność, zbierać naciśnięcia klawiszy i kraść ważne informacje.

- Cyberszpiedzy często szukają **luk w oprogramowaniu lub systemach**, które nie zostały załatane. Luki te stanowią tylne wejście dla hakerów, umożliwiając im penetrację sieci i pobieranie poufnych informacji.

- **Inżynieria społeczna - manipulowanie ludźmi w celu uzyskania poufnych informacji. Cyberszpiedzy mogą podszywać się pod zaufane osoby lub podmioty, aby nakłonić pracowników do zapewnienia dostępu do zastrzeżonych obszarów sieci.**

- Zaawansowane trwałe zagrożenia (APT) - długotrwałe i ukierunkowane cyberataki, w których intruz uzyskuje dostęp do sieci i pozostaje niewykryty przez długi czas. Celem jest ciągłe pozyskiwanie cennych informacji bez uruchamiania alarmów lub bycia wykrytym.

Szpiegostwo

Art. 130. - [Szpiegostwo] - Kodeks karny.

Art. 130. [Szpiegostwo]

§ 1. Kto bierze udział w działalności obcego wywiadu albo działa na jego rzecz, przeciwko Rzeczypospolitej Polskiej,

podlega karze pozbawienia wolności na czas nie krótszy od lat 5.

§ 2. Kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, udziela temu wywiadowi wiadomości, której przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej,

podlega karze pozbawienia wolności na czas nie krótszy od lat 8 albo karze dożywotniego pozbawienia wolności.

§ 3. Kto zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej albo w celu udzielenia obcemu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, gromadzi je lub przechowuje lub wchodzi do systemu informatycznego w celu ich uzyskania,

podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 4. Kto działalność obcego wywiadu, o której mowa w § 1, organizuje lub nią kieruje,

podlega karze pozbawienia wolności na czas nie krótszy od lat 10 albo karze dożywotniego pozbawienia wolności.

§ 5. Funkcjonariusz publiczny oraz osoba pełniąca dyspozycyjnie terytorialną służbę wojskową, dopuszczający się czynu, o którym mowa w § 1,

podlega karze pozbawienia wolności na czas nie krótszy od lat 8 albo karze dożywotniego pozbawienia wolności.

§ 6. Kto bierze udział w działalności obcego wywiadu nieskierowanej przeciwko Rzeczypospolitej Polskiej prowadzonej na jej terytorium bez zgody właściwego organu udzielonej na podstawie odrębnych przepisów,

podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 7. Kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, dokonuje dywersji, sabotażu lub dopuszcza się przestępstwa o charakterze terrorystycznym,

podlega karze pozbawienia wolności na czas nie krótszy od lat 10 albo karze dożywotniego pozbawienia wolności.

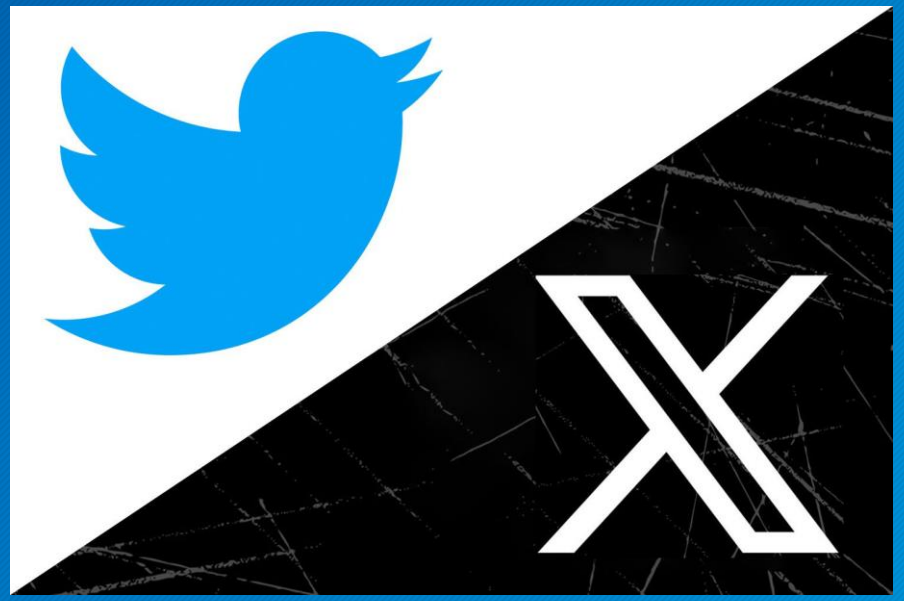
§ 8. Kto czyni przygotowania do przestępstwa określonego w § 7,

podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 9. Kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, prowadzi dezinformację, polegającą na rozpowszechnianiu nieprawdziwych lub wprowadzających w błąd informacji, mając na celu wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczpospolita Polska albo skłonienie organu władzy publicznej Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczpospolita Polska, do podjęcia lub zaniechania określonych czynności,

podlega karze pozbawienia wolności na czas nie krótszy od lat 8.

Zwyczajni szpiedzy



VEGA

INTELLIGENCE

AGENDA

- SZPIEDZY
- **CYBEROPERACJE**
- POSTAWA OBYWATELSKA

VEGA
INTELLIGENCE

Atak na Kyivstar

12 grudnia 2023 r. ujawniono jeden z najpoważniejszych cyberataków na Ukrainie od momentu rosyjskiej inwazji z 24 lutego 2022 r.

W jego wyniku nastąpiło bardzo poważne zakłócenie świadczenia usług przez jednego z największych telekomów ukraińskich Kievstar (szacowana liczba klientów około 24 -26 mln).

Doszło do wyłączenia łączności głosowej oraz dostępu do internetu.

Atak został przeprowadzony przy użyciu zaawansowanych technik hackingowych, w tym ataków typu:

- phishing,
- exploitów (techniki ataku wykorzystujące błędy w oprogramowaniu),
- prób przejęcia kontroli nad systemami firmy.

Kyivstar dopiero po tygodniu od ataku przywrócił mobilny internet i roaming międzynarodowy na całej Ukrainie.

Jeszcze później wróciły inne usługi - w tym łączność stacjonarna, połączenia głosowe i SMS-y.

Straty właściciela operatora Kievstar - firmy VEON oszacowano na 95 mln dolarów.

Cytaty za „Kyiv Post”:

- *sklepy w całym kraju nie mogły obsługiwać płatności kartami płatniczymi,*
- *nie działało wiele bankomatów,*
- *przestało działać automatyczne sterowanie ruchem ulicznym we Lwowie,*
- *były problemy z ostrzeganiem o rosyjskich nalotach,*
- *w tym samym czasie ukraiński bank Monobank stał się celem ataku typu Distributed Denial of Service (DDoS), zakłócając dostęp do strony internetowej banku i usług bankowych.*

Illia Vitiuk – szef cyberdepartamentu Służby Bezpieczeństwa Ukrainy:

… „atak zniszczył „prawie wszystko”, w tym tysiące wirtualnych serwerów i komputerów stacjonarnych – całkowicie zniszczył rdzeń operatora telekomunikacyjnego…

… Na razie możemy śmiało powiedzieć, że atakujący byli w systemie IT Kyivstar co najmniej od maja 2023 roku” (…) mieli pełny dostęp prawdopodobnie przynajmniej od listopada 2023 …

Kyivstar jest własnością holenderskiej firmy telekomunikacyjnej i technologicznej Veon Holdings BV.

Pośrednio jej właścicielami są: **Michaił Fridman**, oraz **Andrei Kosogow.**

Ich działalność biznesowa na świecie jest silnie powiązana z rosyjskimi służbami wywiadowczymi.

W Hiszpanii i Wielkiej Brytanii postawiono im zarzuty związane z udziałem w przestępczości zorganizwanej.

Atak na tak dużą skalę wymaga przygotowania oraz zaangażowanie bardzo dużych sił i środków.

Bardzo niewiele organizacji ma takie możliwości.

Istotne (a czasem kluczowe)
jest posiadania źródła wewnątrz organizacji.

STUXNET

Stuxnet to złośliwy robak komputerowy wykryty po raz pierwszy w 2010 r. i przypuszcza się, że jest rozwijany co najmniej od 2005 r.

Stuxnet atakuje systemy kontroli nadzorczej i gromadzenia danych i uważa się, że jest on odpowiedzialny za spowodowanie znacznych szkód w irańskim programie nuklearnym w ośrodku w Natanz.

W przypadku ośrodka w Natanz celem były tzw. kaskady wirówek do uzyskiwania wzbogaconego uranu – izotopu U235.

Działanie Stuxnet spowodowało, że wirujące części kaskad tzw. centryfugi przekraczyły dopuszczalne prędkości obrotowe i „masowo” ulegały uszkodzeniom.

Dostępne są szacunki, które mówią o zniszczeniu w ten sposób około 20% wirówek.

Dodatkowo zainfekowano około 200 tys. komputerów, a fizyczne uszkodzenia dotknęły około 1000 maszyn.

Kaspersky Lab stwierdził, że wyrafinowany atak mógł zostać przeprowadzony jedynie „przy wsparciu państwa narodowego”.

Z dostępnych opinii ekspertów, w tym amerykańskich, wynika, że wzbogacanie uranu w Natanz zostało zakłócone jedynie na krótko.

Iranowi dość szybko udało się wymienić uszkodzone urządzenia (900 – 1000 sztuk).

Program jądrowy jest kontynuowany nadal.

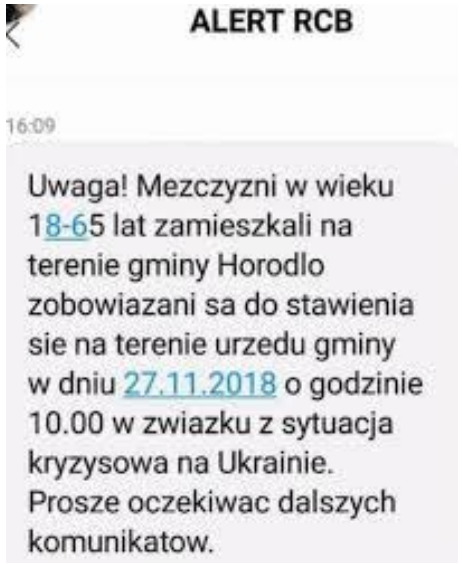
Fake sms

Analiza przypadku

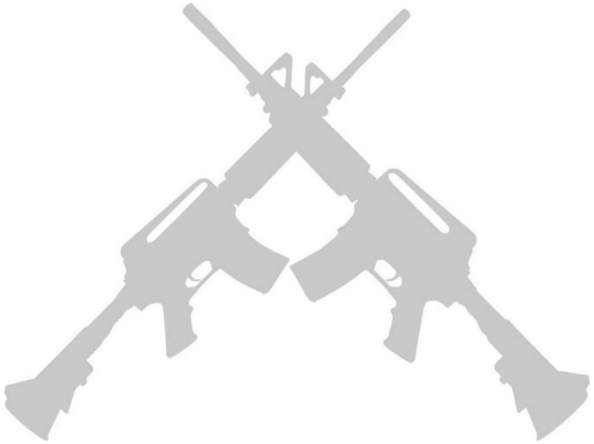
RCB
Rządowe Centrum Bezpieczeństwa

W listopadzie 2018 roku do niektórych mieszkańców gminy Horodło na Lubelszczyźnie oraz gminy Dukla na Podkarpaciu, rozesłano komunikaty – rzekomo z Rządowego Centrum Bezpieczeństwa (RCB)

o następującej treści:



Uwaga! Mezczyzni w wieku 18-65 lat zamieszkali na terenie gminy Horodlo zobowiązani sa do stawienia sie na terenie urzedu gminy w dniu 27.11.2018 o godzinie 10.00 w zwiazku z sytuacja kryzysowa na Ukrainie. Prosze oczekiwac dalszych komunikatow”.

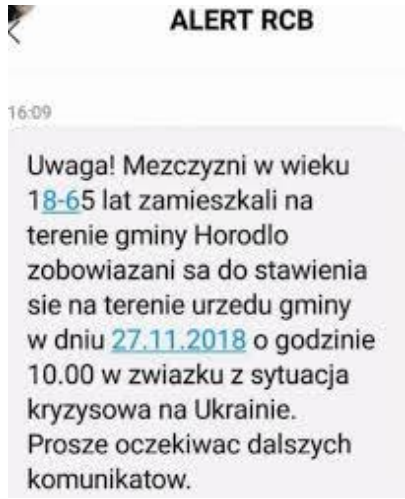


Wkrótce po tym zdarzeniu, Rządowe Centrum Bezpieczeństwa przesłało informacje na telefony komórkowe do wszystkich mieszkańców obu województw, że RCB nie wysłało żadnego alertu w sprawie zgłaszania się mężczyzn do urzędów gmin.

Ocena wiarygodności

Tekst napisany niestarannie:

- błędy ortograficzne (gminy Horodlo)
- literówki i brak polskich znaków (Horodlo, mezczyzni itp.)
- brak jakiejkolwiek wzmianki o mobilizacji w mediach ogólnopolskich i lokalnych



Możliwe cele PRAWDZIWEGO nadawcy

- Jak zareaguje społeczeństwo lokalne?
- Jakie działania podejmą organy samorządowe?
- Czy temat podchwycą media?
- Jak szybko zareaguje RCB?
- Czy sprawa ta i późniejsze, również fałszywe, wielokrotne wezwania mobilizacyjne, nie mają na celu „stępienia” wrażliwości społecznej na podobne wezwania?

Gra na emocjach

- Poczucie obowiązku (gotowość do obrony kraju, domu, bliskich)
- Strach (o siebie, o bliskich, o miejsce pracy, o przyszłość)
- Lekceważenie potencjalnego zagrożenia
- Brak refleksji nad wiarygodnością newsa (niskoenergetyczne przetwarzanie informacji tj. wg podanego w cyberprzestrzeni gotowego wzorca)
- Obojętność

AGENDA

- SZPIEDZY
- CYBEROPERACJE
- **POSTAWA OBYWATELSKA**

Jak reagować?

Przestępcze działania obsych służb i ich agentów mogą mieć ogromne konsekwencje.

- **Zaufaj intuicji, opieraj się na faktach**
- **Zachowaj spokój i kontroluj emocje**
- **Zachowaj ostrożność w kwestii technologii i komunikacji**
- **Dokumentuj zachowanie i rozmowy**
- **Unikaj przekazywania informacji**
- **Nie próbuj działać na własną rękę / Zgłoś sprawę odpowiednim służbom lub przełożonym**
- **Ogranicz kontakt bezpośredni, gdy to możliwe**

Jak rozpoznać?

- Nadmiarowe zainteresowanie szczegółami
- Nietypowe zachowanie i izolacja
- Regularne podróże i niejasne wyjaśnienia
- Tajemnicze użycie technologii
- Nieuzasadnione zainteresowanie procedurami bezpieczeństwa
- Nietypowe zasoby finansowe

fundacja instytut

CYBERBEZPIECZEŃSTWA