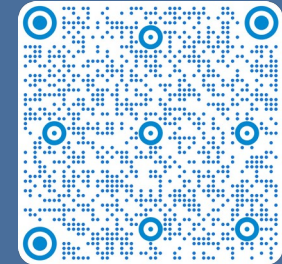


SEKKURA SP. z o.o.

OFERTA



**szkoleń z zakresu bezpieczeństwa
informacyjnego, teleinformatycznego
i fizycznego**

Wprowadzenie

Informacja stanowi współcześnie kluczowy komponent strategiczny dla podmiotów gospodarczych prywatnych i państwowych, jest ona istotnym czynnikiem wytwórczym, coraz częściej postrzegana jest i szacowana jako zasób cenniejszy od środków ekonomicznych.

Celem działań firmy **Sekkura Sp. z o.o.** jest określenie silnych stron i luk w zakresie bezpieczeństwa, aby w jak największym stopniu chronić przedsiębiorstwo przed utratą tych najważniejszych dla interesów przedsiębiorstwa zasobów.

Oferujemy pakiet autorskich, unikatowych szkoleń

Nasza kadra to emerytowani oficerowie i inni funkcjonariusze służb dyspozycyjnych, wykładowcy Uniwersytetu Warszawskiego, Warszawskiego Uniwersytetu Medycznego oraz eksperci w zakresie ratownictwa medycznego i instruktorzy samoobrony z wieloletnim stażem.

Nasza oferta szkoleniowa obejmuje obecnie:

I. Szkolenia

Wstępne szkolenie z zakresu unikania podsłuchów

Bezpieczna komunikacja przez telefon i Internet
Jak nie dać się zhakować lub podsłuchać?

Bezpieczne przechowywanie informacji (komputer i smartfon)
Jak zachować swoją prywatność?

Skuteczne pozyskiwanie i techniki oceny wiarygodności
informacji

Środki i metody inwigilacji elektronicznej - wykład poglądowy

Metodyka pozyskiwania wiedzy i analizy informacji

Biały, szary i czarny wywiad w Internecie

Tajniki Internetów

Terroryzm przemysłowy

Pierwsza pomoc przedmedyczna i autopomoc

Taktyka i procedury bezpieczeństwa

II. Kursy realnej samoobrony

Trening umiejętności praktycznych

Trening umiejętności
psychologicznych

Aspekty formalno-prawne

I.1 Wstępne szkolenie z zakresu unikania podsłuchów

Proponowany zakres szkolenia

Zasady postępowania podczas rozmów biznesowych prowadzonych poza budynkiem firmy

Pokaz urządzeń podsłuchowych

Metody i urządzenia stosowane do wykrywania podsłuchu

Postępowanie z telefonami komórkowymi i laptopami

Zasady rozmów prowadzonych poza obiektami firm

Czas trwania: ok. 120 minut

I.2 Bezpieczna komunikacja przez telefon i Internet.

Jak nie dać się zhakować lub podsłuchać?

Przegląd zagrożeń bezpieczeństwa komunikacji

Metody kradzieży tożsamości i naruszania prywatności

Człowiek jako najsłabsze ogniwo (*phishing / spearphishing*)

Autorski przegląd programów naruszających prywatność

Zabezpieczanie komputerów

Podstawy bezpiecznej i anonimowej komunikacji

Freenet oraz Freenet w trybie Darknet - narzędzie konspiratorów

Anonimowy e-mail

Bezpieczny chat

Anonimowość w Internecie

Generowanie, hodowla lub kupno fałszywych tożsamości

Zabezpieczanie telefonów komórkowych

Metody podsłuchu telefonów komórkowych

Podsłuch telefonów komórkowych - jak robią to profesjonaliści

Dedykowane programy umożliwiające podsłuch

Przegląd systemów bezpiecznych

Bezpieczne korzystanie z Internetu w smartfonie

Bezpieczny sms

Rozmowy telefoniczne bez podsłuchu

Warsztaty: diagnostyka oraz zabezpieczenie własnych telefonów

I.3 Bezpieczne przechowywanie informacji (komputer i smartfon). *Jak zachować swoją prywatność?*

Techniki pozyskiwania jawnych i ukrytych danych systemowych

Dane jawne

Poczta - analiza nagłówek e-mail

Dokumenty elektroniczne

Pliki tymczasowe

Partycje i pliki wymiany

Piki kopii

Logi i rejestry

Dane przeglądarki

Pliki kolejkowania wydruku

Dane ukryte

Metadane

Dane skasowane

Slack space

RAM-slack

Kwestie prawne
tzw. paragrafy hakerskie
w Kodeksie Karnym
(art. 267, 269a i 269b)

Zagrożenie inwigilacją offline. Odnajdywanie zgubionych/zapomnianych haseł do plików

Pozyskiwanie dostępu do systemu operacyjnego bez hasła
Keyloggery sprzętowe

Zaawansowane metody łamania prywatności

Przechwytywanie emisji elektromagnetycznej

Podśluch laserowy

Emisja radiowa

Emitowane ciepło

Technologia ultradźwięków

Sprzątanie po sobie elektronicznych śmieci i zacieranie śladów. Metadane - cichy zabójca prywatności. Metody zautomatyzowanego usuwania metadanych. Czyszczenie pamięci podręcznej i innych śladów. Ukrywanie informacji w plikach: steganografia, steganofonia, steganowizja. Kilka słów o hasłach. Jak skutecznie pozbyć się danych)? Ukrywanie i szyfrowanie plików i katalogów.

I.4 Skuteczne pozyskiwanie i techniki oceny wiarygodności informacji

Techniki i taktyki ewaluacji wiarygodności informacji

Paradoksy i meandry ludzkiej pamięci

Wiarygodność świadków

Anatomia kłamstwa

Sztuka skutecznego kłamstwa

Wykrywanie kłamstwa

Sposoby pozyskiwania prawdy

Źródła rzeczowe informacji

Taktyki i techniki przesłuchań

Gry informacyjne

Efekt błędnej informacji

Pamięć generatywna

Amnezja psychogenna

Ograniczone przetwarzanie bodźców

Obronność percepcyjna

Od psychologicznych sztuczek do wariografu, skopolaminy i tortur

Kształcenie praktycznych umiejętności zdobywania informacji i wyciągania wniosków

Typologia źródeł informacji

Źródła danych (przedmiotowo)

media „klasyczne”

Publicznie dostępne rejestry i ewidencje oraz Internet

Źródła danych (podmiotowo)

II sektor

III sektor

I sektor

Osobowe źródła informacji

Wywiad gospodarczy i paradygmat *competitive intelligence*

Czas trwania części teoretycznej – 240 minut ćwiczenia – 180 minut

I.5 Środki i metody inwigilacji elektronicznej – wykład poglądowy

Typowe miejsca i sposoby inwigilacji.

Urządzenia i oprogramowanie szpiegowskie.

Minikamery i rejestratory audio/wideo.

Lokalizatory GPS.

Podśluch i lokalizacja telefonu.

Podśluchy i odbiorniki.

Generatory szumu / zagłuszacze / szyfrowanie rozmów telefonicznych.

Metody inwigilacji *offline*

Czas trwania: 180 minut

Typologia stanów bezpieczeństwa informacyjnego.

Autorska typologia ryzyk utraty informacji – szpiegostwo przemysłowe i szpiegostwo polityczne.

„Ojciec” podśluchów – „Złotousty”
1945/1952

Polskie „afery podśluchowe”

Restauracja „Sowa
i Przyjaciele” / Pałac
Sobańskich

Restauracja „Różana”

„Afera taśmowa” Renaty
Beger

Studium przypadku zaawansowanej gry operacyjnej – Gazociąg Transsyberyjski, 1982

I.6 Metodyka pozyskiwania wiedzy i analizy informacji

Podejście ilościowe i jakościowe w pozyskiwaniu informacji.

Analiza danych: techniki ilościowe, techniki jakościowe.

Metoda delficka, Burza mózgów (*brainstorming*), Synektyka W.J.J. Gordona, Metoda morfologiczna, Techniki CERMA, Metoda scenariuszowa.

Metody „analogowe”.

Forecasting i foresighting.

Metody symulacyjne.

Metody „liczbowe”: m.in. test Grafa, kryterium Chauveneta, prawo Benforda. Gry symulacyjne i decyzyjne (*serious games*).

Praktyczne aspekty wyboru i oceny operatów losowania. Typy reprezentatywności i metody jej zapewnienia. Wielkość próby a rozkład normalny. Maksymalny standardowy błąd oszacowania.

Testy losowości próby. Problem pseudopredziału ufności Grzegorza Lissowskiego. Poziomy pomiaru - skala S.S. Stevensa.

Interpretacje danych tabelarycznych i miar statystyki opisowej.

Wybrane miary tendencji centralnej i dyspersji.

Wybrane miary związku między zmiennymi: współczynnik korelacji R Pearsona, η^2 (n), chi-kwadrat (χ^2) Pearsona, współczynnik

I.7 Biały, szary i czarny wywiad w Internecie

Topografia Internetu. Wyszukiwanie w Google, zasady indeksowania i pozycjonowania (PageRank). Przegląd wyszukiwarek internetowych. Metawyszukiwarki i multiwyszukiwarki. Wyszukiwarki naturalne. Katalogi internetowe. Wyszukiwarki ludzi. Archiwa Internetu. Inne wyszukiwarki (naukowe, domen, etc.). Wyszukiwanie w Sieci 2.0 – blogów, wyszukiwanie w sieciach społecznościowych i forach dyskusyjnych. Delokalizacja wyników wyszukiwania

Zaawansowane techniki wyszukiwania – Google, Yandex, Bing, DuckDuckGo Hacking.

Google Hacking Database.
Google Hacking jako biały, szary i czarny wywiad

Biały wywiad: wyszukiwanie stron usuniętych i archiwalnych, niektórych informacji o użytkownikach oraz innych informacji

Szary wywiad: zdobywanie informacji o strukturze witryn internetowych oraz parametrów konfiguracyjnych serwerów www

Czarny wywiad: uzyskiwanie informacji zabezpieczonych, osobowych danych wrażliwych, parametrów konfiguracyjnych programów i urządzeń

Tworzenie zapytań prostych i złożonych, porównywanie wyników wyszukiwań, praktyczne poznawanie ograniczeń i możliwości poszczególnych wyszukiwarek internetowych.

Narzędzia do masowego przeszukiwania Internetu: Oryon OSINT Browser, Maltego Paterva.

Eksploracja Internetu Rzeczy (Internet of Things) – Shodan i Censys. Eksploracja ukrytych Internetów: TOR (*The Onion Router*), Freenet, I2P (*Invisible Internet Project*), Zeronet. Alternatywne światy – OpenNIC.

I.8 Tajniki Internetów

Internet czy Internety?

Od Sieci 0.0 do Sieci 5.0. Czy za swojego życia zawrzesz znajomość z myślącym i czującym programem?

Zasoby niewidoczne w Google – dlaczego przeciętny użytkownik Internetu ma dostęp do tylko jednego procenta zasobów Internetu?

Sztuka wyszukiwania w Google – *Google Hacking/Google Dorks*. *Google jako cudowna broń* – od wyszukiwania stron usuniętych i archiwalnych do wyszukiwania kamer i haseł użytkowników

Jak skutecznie inwigilować swoich (nie)przyjaciół? Wprowadzenie do Maltego i Oryon OSINT Browser.
Kilka słów o wirtualnych marionetkach (*sockpuppets*)

Dlaczego bać się Internetu Rzeczy (*Internet of Things*)?
Co nieco o niektórych narzędziach podglądaczy i cyberterrorystów (Shodan, Censys)

Dinozaury Internetu, czyli o tym, co było przed www (wybrane przykłady: BBS/Fidonet, Gopher, Usenet...)

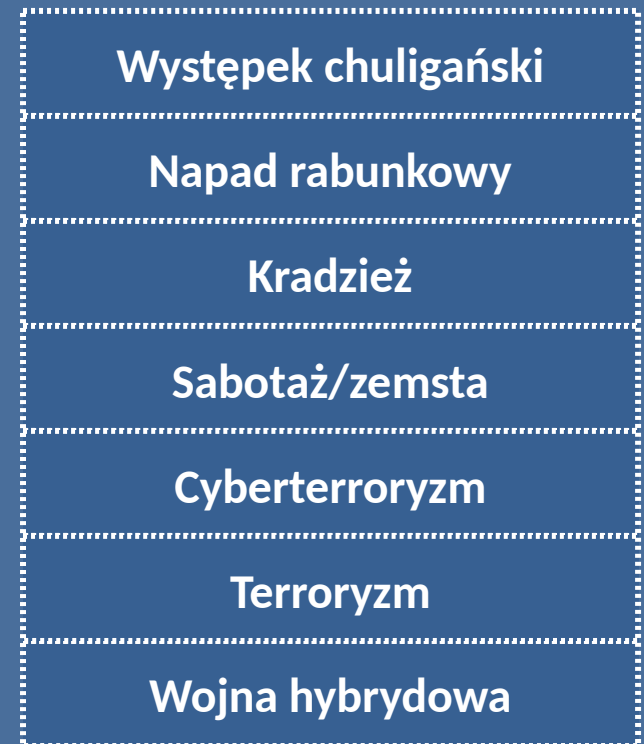
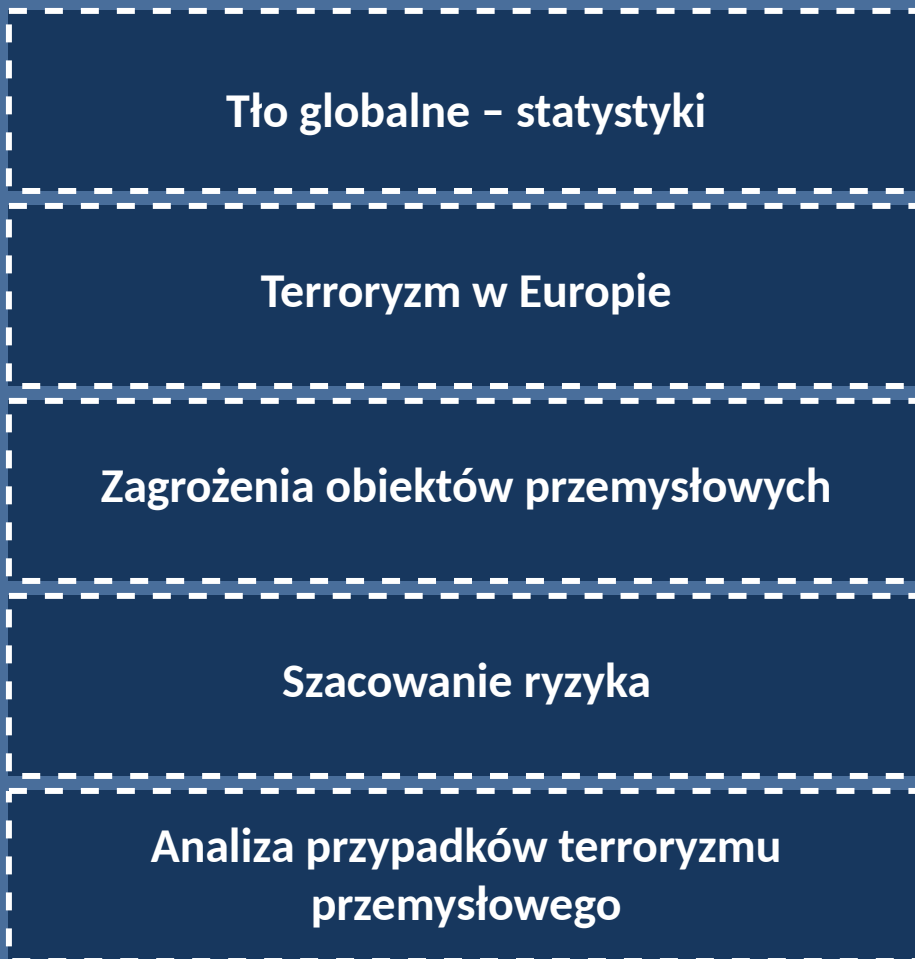
Alternatywny wszechświat. Internet istniejący obok powszechnie znanego – OpenNIC (*Alternative Top Level Domain*)

Jak znaleźć to, czego lepiej nie widzieć (*The Onion Router*), czyli rzecz o Głębokim Internecie (*Deep Web*), gdzie odnajdziemy czarny i czerwony rynek (handel bronią, żywym towarem, narkotykami i płatnych zabójców...) Słowo o równie złych braciach TORa – I2P i Freenet

Cyberhigiena... czyli jak się skutecznie zabezpieczyć korzystając z Internetu? Anonimowi w Internecie – czy wystarczy Linux Tails?

Czas trwania: 180 minut

I.9 Terroryzm przemysłowy



Czas trwania: 120 minut

I.10 Pierwsza pomoc przedmedyczna i autopomoc

Zasady powiadamiania służb ratunkowych o zaistniałych sytuacjach

Podstawowe zasady udzielania pierwszej pomocy przedlekarskiej w przypadku pacjenta urazowego i nieurazowego

Postępowanie w przypadkach zatruc chemicznych, porażen prądem elektrycznym itp.

Prowadzenie reanimacji przez jedną i dwie osoby

Postępowanie w przypadkach szczególnych

Wykorzystanie etatowych i nieetatowych środków do ratowania życia lub zdrowia

Procedury Basic Life Support – BLS /fantom/

Zasady wykorzystania AED

Pokaz sytuacji symulowanej – zdarzenie

Czas trwania: ok. 2 x 55 minut, ćwiczenia – 50 minut

I.11 Taktyka i procedury bezpieczeństwa

- Zagrożenia związane ze specyfikacją wykonywanego zawodu i obecne zagrożenia firmy przestępczością
- Sposoby działania przestępców, ich wyposażenia, uzbrojenie, zasady zapamiętywania faktów, cech szczególnych i wyposażenia
- profilaktyka i prewencyjne działania mające na celu zwiększenia stopnia bezpieczeństwa firmy
- Zachowanie podejrzane, agresywne klientów w szczególności pod wpływem środków psychodelicznych, alkoholu, narkotyków, dopalaczy ...
- Bójka klientów, napad/rozbój
- Pożar
- Sabotaż, podejrzana przesyłka, awaria techniczna
- Grupy pseudokibiców
- Klienci zabarykadowani w toalecie/łazience, uprawianie seksu przez klientów w toalecie/łazience
- Użycie broni
- Próby podpalenia
- Opieszła interwencja służb – policji/straży miejskiej

Czas trwania: ok. 2 x 55 minut, wykład z prezentacją, 55 minut – ćwiczenia praktyczne w postaci symulacji napadu i odbicia zakładników

II Kursy realnej samoobrony...

Oferujemy dedykowane, wieloaspektowe kursy realnej samoobrony uwzględniające faktyczne uwarunkowania psychofizyczne uczestników

Pełny program kursu obejmuje następujące aspekty

Trening umiejętności praktycznych

Trening umiejętności psychologicznych

Aspekty formalno-prawne

Ogniskujemy się na potrzebach grup, szczególnie zagrożonych incydentami bezpieczeństwa, oferując trzy warianty szkoleń

Samoobrona dla kobiet

Samoobrona dla seniorów

Samoobrona dla menedżerów/biznesmenów

Optymalny czas trwania kursu: dwudniowy, prowadzimy również kursy ciągłe w wymiarze 30 i 60 godzin, a także krótkie prezentacyjne briefingi w wymiarze kilkugodzinnym

II.1 Trening umiejętności praktycznych

Techniki samoobrony



tzw. punkty wrażliwe
(*atemi waza*)

Wybrane rzuty, dźwignie, duszenia i trzymania dostosowane do kondycji psychofizycznej ćwiczącego

Specyfika walki w różnym otoczeniu

W pomieszczeniach o małej kubaturze, na otwartej przestrzeni, przy słabym oświetleniu, podłożu utrudniającym utrzymanie równowagi, etc.

Wykorzystanie w samoobronie broni białej oraz improwizowanej

Techniki samoobrony za pomocą gazu pieprzowego, paralizatora, yawary/kubotanu, pałki teleskopowej

Walka bez broni

(ofensywna i defensywna obrona przed chwytami i trzymaniami – z przodu, z tyłu, z boku, jednorącz i oburącz, za ręce, włosy, etc.), obrona przed uderzeniem pięścią, kopnięciem, duszeniem, obrona przed wieloma przeciwnikami, obrona przed atakiem bronią białą / improwizowaną, obrona przed szantażem bronią palną i białą w tym improwizowaną (strzykawką, butelką), walka na ziemi (*ne waza*)

II.2 Trening umiejętności psychologicznych

Typologia i statystyka zagrożeń
poszczególnych grup

Kradzież, rozbój, rabunek, napad
rabunkowy, pobicie, gwałt i inne
nadużycia seksualne, sytuacja zakładnicza

Wiktymologia

Co nauka może nam doradzić, by nie stać się
ofiara przestępstwa
(trening umiejętności interpersonalnych, reguły
zachowania w zależności od sprawców:
atakujący vs szantażujący bronią, sprawca
trzeźwy vs pod wpływem środków
psychoaktywnych, etc.)

Jak nie dopuścić do ataku
- reguły psychotechniczne

Profilowanie sprawców przestępstw przeciwko
mieniu, zdrowiu i życiu
- cechy socjopsychodemograficzne

Symptomy niebezpieczeństwa

Sztuka obserwacji i interpretacji sygnałów
potencjalnego incydentu bezpieczeństwa

Socjopsychologiczne reguły skutecznego wzywania pomocy.

Ucieczka - jeśli tak, to jak to uczynić najskuteczniej

Wiarygodność świadków Portret pamięciowy

Jak być dobrym świadkiem - zasady składania zeznań
i przesłuchań, paradoksy i meandry ludzkiej pamięci:
ograniczone przetwarzanie bodźców, efekt błędnej
informacji, obronność percepcyjna, amnezja psychogenna,
pamięć generatywna

II.3 Aspekty formalno-prawne

Charakterystyka, zakres i niuanse obrony koniecznej
– czyli jak się bronić bez obaw o odpowiedzialność karną

Broń i inne narzędzia niebezpieczne
– czyli co dozwolone, a co zakazane przez polskie prawo

Typy broni, obrażenia, statystyki medyczne
– prezentacja i omówienie typowych narzędzi przestępstw przeciwko życiu i zdrowiu i potencjalnych skutków ich użycia

Korzystamy z doświadczeń i możliwości, jakie oferują rozmaite sztuki i sporty walki, jednak ogniskujemy się na najskuteczniejszej ze sztuk (w naszej opinii), wdrożonej jako system samoobrony w licznych policjach i armiach świata – Jiu-Jitsu

Zajęcia prowadzą doświadczeni, dyplomowani instruktorzy samoobrony

Nasz zespół szkoleniowy



Paweł Tomczyk – absolwent Wojskowej Akademii Technicznej i Akademii Sztabu Generalnego (kierunek: rozpoznanie), wyższy oficer Wojska Polskiego (przeniesiony do rezerwy), służbę odbywał w jednostkach liniowych wojsk zmechanizowanych, a następnie w IC MON. Brał udział w misji SFOR w Bośni i Hercegowinie. Specjalista w zakresie ochrony informacji niejawnych. Instruktor sztuk walki (2 dan Shizoku-Ryu Jiu-Jitsu oraz 3 dan Modern Ju-Jitsu), posiadacz licencji detektywistycznej oraz patentu jachtowego sternika morskiego. Aktualnie członek zarządu i współwłaściciel firmy Sekkura.



Gabriela Kamińska – absolwentka Wydziału Zarządzania Akademii Ekonomicznej Katowicach oraz studiów podyplomowych na Wydziale Wychowania Fizycznego w Warszawie. Instruktor rekreacji ruchowej w specjalności samoobrona (1 dan Modern Jiu-Jitsu oraz 1 kyu Shizoku-Ryu Jiu-Jitsu). Prowadząca i współprowadząca licznych szkoleń z zakresu zachowania w sytuacjach krytycznych oraz pierwszej pomocy przedmedycznej. Prowadzi sekcję sztuk walki w Nowym Dworze Mazowieckim. Uprawia szermierkę i żeglarstwo.

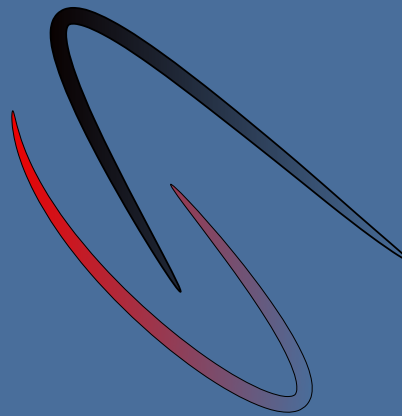


Daniel Mider – doktor nauk humanistycznych w zakresie nauk o polityce (2008, *summa cum laude*). Wykładowca Uniwersytetu Warszawskiego i Szkoły Głównej Handlowej, adiunkt w Zakładzie Socjologii i Psychologii Polityki INP UW, kierownik Pracowni Metodologii Badań Politologicznych. Egzaminator Europejskiego Certyfikatu Umiejętności Komputerowych, certyfikowany informatyk śledczy. Twórca i wykładowca specjalności infobrokering polityczny. Autor licznych publikacji z zakresu socjologii Internetu, socjologii przemocy, metodologii badań oraz partycypacji politycznej. Analityk biegle posługujący się metodami ilościowymi i jakościowymi obróbki informacji. Ekspert UW w zakresie infobrokeringu i cyberterroryzmu.

Zapraszamy do kontaktu

Sekkura Sp. z o. o.

01-445 Warszawa
ul. Erazma Ciołka 13 lok. 114



SEKKURA SP. Z O.O.

www.sekkura.com.pl

E-Mail:

sekkura@sekkura.com.pl

Telefon:

+48 517 278 168