Materiały pokonferencyjne

# Analiza kryminalna w przyszłości

Norway grants

CENTRALNE BIURO ANTYKORUPCYJNE CBA

LEAF.2022
law enforcement analysis of the future

Materiały pokonferencyjne

# Analiza kryminalna w przyszłości

Projekt „Wzmocnienie kompetencji organów ścigania i wymiaru sprawiedliwości w obszarze analiz: kryminalnej i strategicznej, wspomagających proces rozpoznawania, zwalczania i zapobiegania korupcji oraz przestępczości gospodarczej” finansowany ze środków Norweskiego Mechanizmu Finansowego 2014-2021

Warszawa 2023

**CENTRALNE BIURO ANTYKORUPCYJNE**
Al. Ujazdowskie 9
00-583 Warszawa
**www.cba.gov.pl**

**Opracowanie:**
Departament Analiz CBA

Elektroniczna wersja:
www.cba.gov.pl – w dziale „Publikacje”

**ISBN 978-83-949606-4-3**

**Opracowanie graficzne, korekta, przygotowanie do druku oraz druk**
Wydział Wydawnictw i Poligrafii Centrum Szkolenia Policji w Legionowie
ul. Zegrzyńska 121, 05-119 Legionowo
www.csp.edu.pl

**Nakład:**
60 egz.

# Spis treści
# Table of contents

# Wstęp

W dniach 26–28 października 2022 r. w Warszawie odbyła się międzynarodowa konferencja LEAF 2022 (Law Enforcement Analysis of the Future), organizowana przez Centralne Biuro Antykorupcyjne. Wydarzenie zrealizowano w dwóch formułach: online oraz stacjonarnie.

Do udziału w wydarzeniu w roli słuchacza lub prelegenta zaproszono przedstawicieli służb, środowiska naukowego i niezależnych ekspertów.

Podczas trzydniowej konferencji LEAF 2022 specjaliści analizy kryminalnej i strategicznej, przedstawiciele świata nauki i praktycy prezentowali swoje prelekcje. Konferencja była okazją do dyskusji oraz poznania perspektywy teoretycznej i praktyki poruszanych zagadnień.

W kolejnych dniach swoje wystąpienia prezentowali:

**26.10.2022 r.**

- dr hab. Wojciech Filipkowski, prof. UwB:
  „Propozycja założeń edukacji analityków strategicznych – przyczynek do dyskusji";
- Beata Wiśnicka-Zawierucha, niezależny ekspert:
  „Pranie pieniędzy w transakcjach korespondenckich";
- Paweł Łukaczyk, KAS:
  „Analiza przestrzenna jako element analizy strategicznej – sposoby wykorzystania w procesie decyzyjnym i działaniach służb";
- dr hab. Piotr Chlebowicz, prof. UWM
  „Strategiczna analiza kryminalna. Implikacje dla bezpieczeństwa państwa";
- dr Agnieszka Butor-Keler, KNF:
  „Przeciwdziałanie nadużyciom na rynku, finansowym – kompetencje i doświadczenia KNF";
- dr Tomasz Michalak, UW:
  „Security games and their applications to defend critical infrastructure";
- Rafał Szczepaniak, UCS we Wrocławiu:
  „Rozwój analizy kryminalnej w ramach modernizacji KAS";
- Karol Drąg, Ministerstwo Finansów:
  „Znaczenie współpracy GIIF z organami ścigania dla tworzenia analiz strategicznych w obszarze przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu".

**27.10.2022 r.**

- dr hab. Marcin Wojtysiak-Kotlarski, prof. SGH:
  „Nowoczesna analiza strategiczna jako szansa na zwiększenie dynamiki rozwoju Polski";
- prof. dr hab. Andrzej Zybertowicz:
  „Agentura, weaponizacja współzależności gospodarczej i cyfrowa degradacja poznawcza: Dlaczego Zachód nie zapobiegł inwazji Moskwy na Ukrainę";
- Radzhami Dzhan, NABU:
  „Anti-corruption authority analytical department: key points";
- Tetiana Vodopianova, NABU:
  „OSINT in objectives of freezing, seizure and confiscation of assets: challenges and difficulties";
- Jarosław Wolski, niezależny ekspert:
  „OSINT jako narzędzie ostrzegające o zbliżającym się konflikcie zbrojnym jako metoda estymowania strat stron konfliktu";
- Giovanni Angelini, Guardia di Finanza:
  „Legal and regulatory framework on assets freezing linked to sanctions to the Russian Federation and Belarus";
- Roberto Ribaudo, Ministero di Interno:
  „Activity of the Italian ARO / CARIN office to implement EU sanctions. Prespectives on a new European legal framework on AROs";
- dr Tomasz Michalak, UW:
  „AI-based solutions for combating financial crime";
- dr hab. Kacper Gradoń, wykładowca akademicki:
  „Sztuczna inteligencja w wojnie hybrydowej – miecz obosieczny".

**28.10.2022 r.**

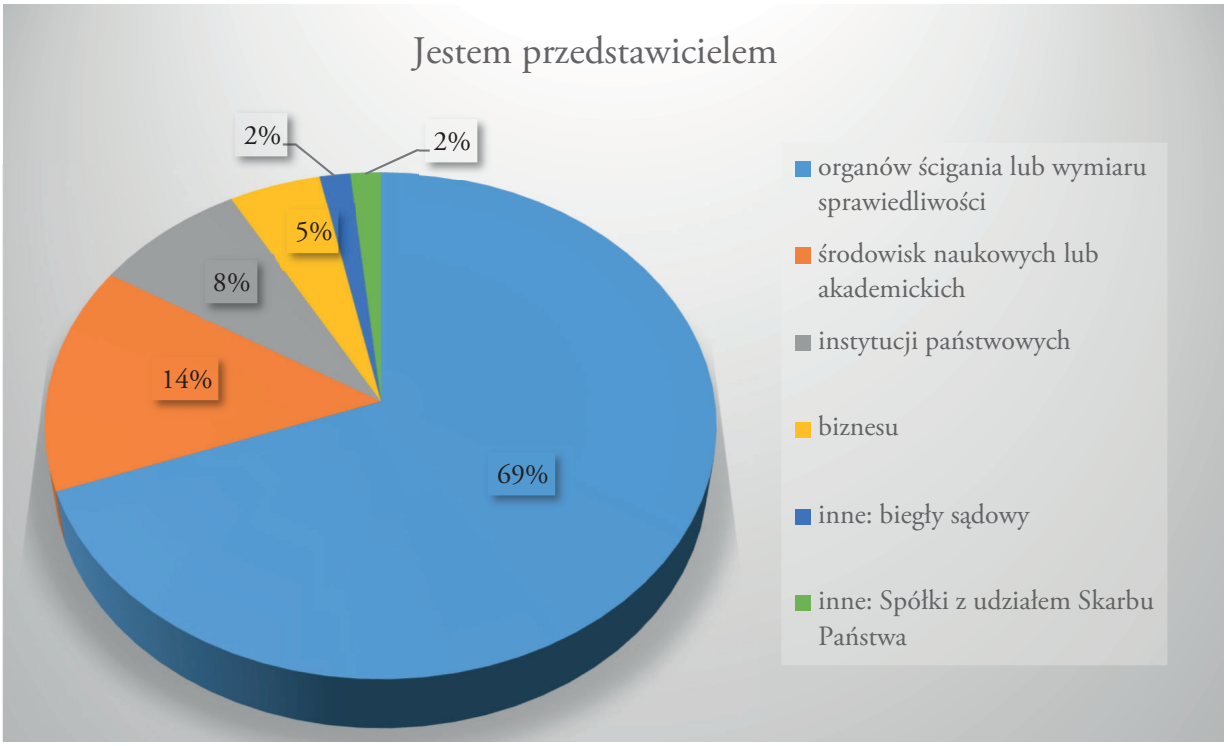
- dr inż. Jacek Dajda, AGH:
  „Od analizy informacji do dezinformacji – współczesne kierunki rozwoju rozwiązań analitycznych realizowanych w ramach Centrum Bezpieczeństwa AGH";
- dr inż. Fryderyk Darnowski, CBA:
  „Od dyskietki do data lab – zmiany w informatyce kryminalistycznej";
- dr Harm van Beek, Netherlands Forensic Institute:
  „Lessons learned from implementing digital forensic as a service";
- Joanna Krupa, CBA:
- „Social trading. Kreatywne metody omijania przepisów ustawy o obrocie instrumentami finansowymi";
- Dominic Maciver, Gareth Crabbe, National Crime Agency:
  „International Anti-Corruption Coordination Centre (IACCC) capabilities to suport grand corruption investigations";
- Matt Caton, Lee Watkins, National Crime Agency:
  „Data exploitation and biometrics";
- Anna Krop, analityk kryminalny:
  „Rzecz w internecie? Czy internet w rzeczy? Przestępczość nowych technologii".


Konferencja była realizowana w ramach projektu pn. „Wzmocnienie kompetencji organów ścigania i wymiaru sprawiedliwości w obszarze analiz: kryminalnej i strategicznej, wspomagających proces rozpoznawania, zwalczania i zapobiegania korupcji oraz przestępczości gospodarczej". Przedsięwzięcie jest finansowane ze środków Norweskiego Mechanizmu Finansowego 2014–2021 w obszarze programowym PA20 „Międzynarodowa współpraca policyjna i zwalczanie przestępczości" w Programie „Sprawy wewnętrzne", przydzielonych w drodze konkursu przez Ministra Spraw Wewnętrznych i Administracji.

Więcej informacji na temat Norweskiego Mechanizmu Finansowania i projektów realizowanych w ramach funduszy norweskich jest dostępnych pod adresami: www.eeagrants.org; www.norwaygrants.org; www.eog.gov.pl; www.fundusze.mswia.gov.pl.

Uczestników konferencji poproszono o wypełnienie krótkiej, anonimowej ankiety celem poznania opinii na temat wydarzenia oraz jego ewentualnej przyszłości. 95 procent badanych uczestników konferencji oceniło wydarzenie bardzo wysoko i wysoko, według uczestników konferencja sprzyjała wymianie wiedzy i doświadczeń, tym samym jej główne cele zostały osiągnięte. Jako najsilniejsze strony konferencji wskazywano dobór tematów i prelegentów. Uczestnicy w ankiecie stwierdzili, że zdecydowanie powinna się odbyć kolejna edycja konferencji uwzględniająca szersze poruszenie tematów analizy kryminalnej oraz informatyki śledczej.

Struktura uczestników konferencji przedstawiała się następująco:




Niniejsza publikacja prezentuje artykuły autorów, którzy zgodzili się przygotować opracowania na kanwie wykładów konferencyjnych.

# Przemówienie Zastępcy Szefa Centralnego Biura Antykorupcyjnego rozpoczynające Konferencję Analizy Kryminalnej i Strategicznej LEAF 2022

**Szanowni Państwo**

*Pragnę powitać szanownych gości na międzynarodowej konferencji analizy kryminalnej i strategicznej. Serdecznie witam partnerów projektu: przedstawicieli Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Prokuratury Krajowej, Ministerstwa Finansów oraz partnerów zagranicznych: Narodowego Biura Antykorupcyjnego Ukrainy oraz Agencji Unii Europejskiej do Spraw Współpracy Organów Ścigania – Europolu.*

*Z góry dziękuję prelegentom, którzy zdecydowali się podzielić z nami swoją cenną wiedzą akademicką oraz praktyczną. Przyczyniają się Państwo do zwiększenia potencjału analitycznego służb zajmujących się zwalczaniem korupcji oraz przestępczości gospodarczej.*

*Witam także słuchaczy, którzy przybyli do nas z całej Polski, Wielkiej Brytanii, Włoch, Portugalii, Czech, Słowacji, Litwy, Bułgarii, Szwecji, Irlandii. Szczególne podziękowania należą się naszym ukraińskim gościom, którzy pomimo trudnych warunków wojennych w swoim kraju zdecydowali się przyjechać do Warszawy i podzielić się z nami swoimi doświadczeniami.*

*Cieszę się, że jesteście tu z nami, i mam nadzieję, że to wydarzenie przyczyni się do wymiany idei oraz dalszego zacieśniania współpracy.*

*Witam także zdalnych uczestników konferencji. Dzięki nowym technologiom pomimo fizycznego dystansu mogą Państwo uczestniczyć w czasie rzeczywistym w tym wydarzeniu, doskonaląc i pogłębiając swoje umiejętności.*

*Mam nadzieję, że zarówno uczestnicy stacjonarni, jak i zdalni wyniosą z wykładów to, co najważniejsze – praktyczną wiedzę oraz inspirację do coraz skuteczniejszego działania w wykrywaniu i zapobieganiu przestępstwom o charakterze ekonomicznym i finansowym.*

*Głównym celem projektu, którego ważną część stanowi nasze dzisiejsze spotkanie, jest wzmocnienie współpracy międzynarodowej, dlatego też zdecydowaliśmy się zaprosić do udziału tak wiele instytucji. Niejednokrotnie realizacja najbardziej skomplikowanych spraw w historii naszego Biura nie byłaby możliwa bez współpracy z naszymi polskimi i zagranicznymi partnerami. Pamiętając o tym, mam nadzieję, że udział w konferencji będzie sprzyjać wzajemnemu poznaniu się, co zaowocuje w przyszłości jeszcze lepszą współpracą. A nic nie integruje ludzi tak, jak wspólny cel i praca w dążeniu do jego osiągnięcia.*

*Zagrożenia, z którymi mamy do czynienia, często mają charakter transgraniczny, chciwość i chęć zysku kosztem innych często łączą przestępców ponad granicami państw i strefami czasowymi. Dlatego cieszę się, że mamy tu na sali przedstawicieli służb i organów ścigania tak wielu krajów. Łączy nas to, że wszyscy działamy na rzecz wykrywania i zwalczania poważnej przestępczości ekonomicznej, która godzi w ład gospodarczy, a ostatecznie i ład społeczny naszych państw, a co za tym idzie – w dużej mierze także w porządek europejski.*

*To, że spotykamy się w centrum Warszawy oraz w centrum Europy, jest w pewnym sensie też symboliczne. W Europie, tuż za naszą granicą, toczy się wojna. Wojna, która dotyka nas wszystkich zarówno*

*w wymiarze ekonomicznym, jak i czysto ludzkim. Jest to także wojna informacyjna, która toczy się w mediach i internecie, a dotyczy tak naprawdę każdego obywatela.*

*Informacja to potężna broń, waluta i jeden z najcenniejszych towarów na świecie. Ten kto wie więcej – wygrywa. Sama informacja jednak nie przekłada się bezpośrednio na wiedzę. Ta bowiem jest informacją przetworzoną, scaloną oraz przede wszystkim zinterpretowaną w kontekście posiadanego uprzednio rozeznania. Mam nadzieję, że wszystko, co Państwo jako uczestnicy tej konferencji usłyszą i czego się nauczą, zaowocuje właśnie konkretną wiedzą, jak systematyzować i interpretować informacje w taki sposób, by jak najpełniej i właściwie je wykorzystać. Dążymy do tego, by informacje stały się wiedzą, a nie jedynie ogromnym zbiorem chaotycznych faktów.*

*Pod takim kątem wybierane były też tematy prelekcji. Zajmiemy się zagadnieniami szeroko rozumianej analizy finansowej i ekonomicznej, zaawansowanymi technikami kryminalistycznymi, nowymi technologiami w służbie analizy kryminalnej i strategicznej, a także obecną sytuacją geopolityczną, ciągle jednak w kontekście zadań stających przed analitykami i organami ścigania.*

*W swojej codziennej pracy analitycy organów ściągania i służb specjalnych mierzą się ze złożonymi zagadnieniami. Najczęściej powtarzającym się argumentem dla ich ciągłego kształcenia jest to, żeby zawsze móc być o krok przed przestępcami, a co za tym idzie, używać metod i narzędzi, które będą skuteczne i efektywne. Tylko w taki sposób będziemy mieli wyrównane szanse w starciu z przeciwnikami. Metody wykorzystywane przez przestępców zarówno do popełniania czynów zabronionych, zacierania ich śladów, jak i do legalizowania środków z nich pochodzących stale ewoluują. Jako służby powinniśmy być zawsze co najmniej krok przed nimi, by nie tylko wykrywać, ale i w pewnym stopniu przewidywać oraz zapobiegać części z nich. Analiza strategiczna i kryminalna jest narzędziem idealnie wręcz skrojonym do tych celów. Daje służbom metody oraz środki, by w sposób systemowy i precyzyjny wskazywać obszary zagrożenia, badać je pod kątem nieprawidłowości, a także określać dalsze kierunki działań operacyjnych i wywiadowczych. I taki jest przede wszystkim cel tej konferencji: poszukiwanie metod, by skutecznie i bez lęku stawiać czoła nowym wyzwaniom, oraz promocja najlepszych praktyk i rozwiązań w zakresie analizy kryminalnej i strategicznej.*

*Jestem głęboko przekonany, że najlepsze rozwiązania rodzą się na styku praktyki oraz akademickiej wiedzy i dlatego bardzo doceniam udział środowiska naukowego w tej konferencji i szczególnie dziękuję pracownikom naukowym, szanownym panom profesorom za obecność. Państwa chęć dzielenia się swoją wiedzą jest w istocie działalnością wybitnie propaństwową.*

*Zachęcam do czynnego udziału we wszystkich trzech dniach wydarzenia, ponieważ każdy z nich będzie miał inną specyfikę oraz wiodącą tematykę, ale niewątpliwie wzajemnie się dopełnią.*

*Zapraszam uczestników stacjonarnych także do uczestnictwa w uroczystej kolacji, która odbędzie się w zabytkowej fortecy, interesującym punkcie na mapie historii Warszawy. Niech to wieczorne spotkanie będzie okazją do wymiany opinii oraz nawiązania kontaktów, które ułatwią nam dalszą współpracę.*

*Daniel Karpeta*
*Zastępca Szefa*
*Centralnego Biura Antykorupcyjnego*

***dr hab. Marcin Wojtysiak-Kotlarski, prof. SGH***

*Kierownik Zakładu Strategii Międzynarodowych*
*Instytut Zarządzania*
*Kolegium Zarządzania i Finansów*
*Szkoła Główna Handlowa w Warszawie*
*ORCID: 0000-0002-2500-7191*

# Nowoczesna analiza strategiczna jako szansa na zwiększenie dynamiki rozwoju Polski – syntetyczna prezentacja głównych tez wystąpienia autora na konferencji LEAF 2022[1]

## Wstęp

Polska jest krajem, którego historia, w tym historia gospodarcza, jest w szczególności bliska naszemu sercu, ponieważ tutaj dane nam było się urodzić, tutaj żyjemy, tu pracujemy, wychowujemy dzieci itd. Mimo że współczesny świat staje się coraz bardziej zintegrowany, jako iż postępuje dynamicznie proces globalizacji będący wielowymiarowym mechanizmem wpływu na codzienne działania i aktywności człowieka, to jednak bardzo ważna jest perspektywa dobrostanu obywateli danego państwa[2].

Mimo rozlicznych organizacji integrujących państwa, czy to na płaszczyźnie politycznej, gospodarczej, kulturowej, czy innych, poszczególne państwa konkurują. Z kolei, szeroka dostępność ludzi w praktycznie każdym zakątku globu, w tym naturalnie w Polsce, do wiedzy i informacji na temat sytuacji społeczno-gospodarczej na całym świecie rodzi niejako nowe powinności. Skoro wiemy, że dany kraj nawiedza ogromna klęska głodu lub tragiczne w skutkach trzęsienie ziemi, reagujemy

---

[1] Inspiracją do powstania tego tekstu są badania prowadzone w Szkole Głównej Handlowej w Warszawie w ramach projektu „Mazowsze akceleratorem globalnych przedsiębiorstw". Jest to projekt finansowany przez Narodowe Centrum Badań i Rozwoju w ramach strategicznego programu badań naukowych i prac rozwojowych „Społeczny i gospodarczy rozwój Polski w warunkach globalizujących się rynków" GOSPOSTRATEG. Głównym celem programu GOSPOSTRATEG jest wzrost wykorzystania w perspektywie do 2028 r. rezultatów badań społeczno-ekonomicznych w kształtowaniu krajowych i regionalnych polityk rozwojowych. Tekst ten w znacznym stopniu nawiązuje również do wystąpienia autora na Międzynarodowej Konferencji LEAF 2022 (*Law Enforcement Analysis of the Future*) odbywającej się w dniach 26–28 października 2022 r., w ramach której eksperci z różnych rejonów Polski i Europy, przedstawiciele środowiska naukowego, służb specjalnych i niezależni eksperci podejmowali między innymi rozmowy na temat analizy strategicznej prowadzonej w kontekście państwa. Wersja tekstu w formie rozszerzonej została opublikowana w: M. Wojtysiak-Kotlarski, *Nowoczesna analiza strategiczna jako szansa na zwiększenie dynamiki rozwoju Polski*, w: *30 lat w naukach społecznych. Nowe myśli i idee*, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2023, s. 541–560. Niniejszy materiał ma formę skróconą wskazanego powyżej tekstu i ma na celu przede wszystkim prezentację głównych tez wystąpienia na konferencji LEAF – przypis autora.

[2] Zobacz szerzej: W. Szymański, *Interesy i sprzeczności globalizacji. Wprowadzenie do ekonomii ery globalizacji*, Wydawnictwo DIFIN, Warszawa 2004.

i pomagamy. W tak zarysowanym kontekście, mimo rozlicznych międzynarodowych współzależności, kryterium skuteczności polityki gospodarczej w aspekcie lokalnym, tj. na szczeblu gospodarki danego państwa, jest nadal bardzo ważne i aktualne.

Przedmiotowy tekst ma charakter głosu w dyskusji na temat tego, co jest istotne, aby można było zwiększyć dynamikę rozwoju polskiej gospodarki. Dążymy do tego, aby rozwój był zrównoważony w wymiarach ekonomicznym, społecznym i środowiskowym[3]. Nie powinno być bowiem tak, przykładowo, że bardzo silne dążenie do uprzemysłowienia będzie realizowane kosztem zdrowia obywateli czy też kosztem zanieczyszczenia środowiska. Nie aspirujemy w żadnym wypadku do tego, aby tekst tu prezentowany miał całościowy charakter. Nie jest możliwe w krótkim artykule poruszyć wszystkie ważne wątki. Niemniej jednak intencją autora jest podzielenie się z szerszą publicznością pewnymi wstępnymi spostrzeżeniami nawiązującymi do prowadzonych badań naukowych i włączenie się tym tekstem w dyskusję na temat tego, jak w sposób nowoczesny prowadzić analizy strategiczne na szczeblu państwa.

## 1. Budowanie strategii na szczeblu państwa – istota i niektóre wyzwania

Zastanawianie się nad strategią rozwoju jest zagadnieniem trudnym, ale o niezwykłej wadze. Strategia wyznacza kierunek, mówi o priorytetach, odpowiada na podstawowe pytania dotyczące przyszłości państwa[4]. Myśląc strategicznie, definiujemy więc pewien plan dotyczący tego, jak chcemy osiągnąć w przyszłości te cele, które przed sobą postawimy.

Formułując strategię na szczeblu państwa, należy pamiętać o tym, że gospodarka z definicji funkcjonuje wobec problemu rzadkości, co oznacza konieczność przyjęcia do wiadomości, że nie da się w gospodarce osiągnąć wszystkiego, czego oczekują interesariusze. Nie da się więc abstrahować od zagadnienia rozliczalności. Nie jest sztuką wydawać pieniądze podatników czy wierzycieli państwa. Sztuką jest robić to w sposób racjonalny ekonomicznie.

W kontekście polskiej gospodarki wielokrotnie definiowano strategie dotyczące gospodarki. Zawsze elementem tych strategii była pewna wizja, tj. docelowy obraz państwa, który chcemy osiągnąć dzięki realizacji danej strategii (planu). Strategia zawiera zdefiniowane cele: niekiedy jest ich niedużo, niekiedy bardzo wiele. Niekiedy są one ambitne i atrakcyjne, praktyka w tym zakresie jest różna. Niekiedy są one mało precyzyjne, czasami trudno kwantyfikowalne. Ważne, żeby były atrakcyjne dla społeczeństwa, ambitne i wykonalne.

## 2. Siła przedsiębiorstw jako wyznacznik siły gospodarki

Charlie Wilson, prezes General Motors, wypowiedział wiekopomne słowa: „Co jest dobre dla naszego kraju, jest też dobre dla General Motors. A co jest dobre dla General Motors, jest też dobre dla Ameryki”[5]. Oczywiście, powyższe stwierdzenie jest pewnym uproszczeniem. Przykładowo, korzyści związane z funkcjonowaniem danego przedsiębiorstwa w różnym stopniu rozkładają się na poszczególne grupy interesariuszy; co więcej, nawet w ramach danej grupy interesariuszy, np. menedżerów lub pracowników, mogą istnieć niekiedy bardzo duże rozpiętości zarobków i dodatkowych benefitów na tych samych stanowiskach.

---

[3] Por. G.W. Kołodko, *Świat w matni. Czwarta część trylogii*, Wydawnictwo Prószyński i S-ka, Warszawa 2022.

[4] Zob. *Strategia na rzecz odpowiedzialnego rozwoju do roku 2020 (z perspektywą do 2030 r.),* https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju, porównaj „Polski ład”, https://www.gov.pl/web/polski-lad/o-programie.

[5] Zobacz: Ch. Leduff, *Detroit. Sekcja zwłok Ameryki*, wyd. 3, Wydawnictwo Czarne, Wołowiec 2019; podaję za: www.polityka.pl, opublikowane 3 marca 2015 r.

Generalnie jednak istnieje dość powszechny pogląd, iż Polska ma ogromy potencjał gospodarczy. Polska gospodarka to obecnie dziewiętnasta największa gospodarka według danych opublikowanych w raporcie *World Economic Outlook Database* przez Międzynarodowy Fundusz Walutowy w październiku 2020 r. Z tego punktu widzenia polskie aspiracje do współkształtowania światowej polityki gospodarczej są uzasadnione.

Po dość chaotycznych przemianach własnościowych okresu transformacji, kiedy prywatyzacja majątku narodowego w wielu przypadkach dokonywała się nazbyt pospiesznie, z brakiem wystarczającego zabezpieczenia interesów państwa polskiego, wyraźnie dostrzegalny jest w ostatnich latach pozytywny trend polegający na zaakcentowaniu znaczenia tego, aby w polskiej gospodarce powstawały firmy-czempiony[6].

Poczynić należy wobec tej sytuacji dwa komentarze. Po pierwsze, nie jest proste, aby w krótkim okresie przebudować system gospodarczy na sposób zasadniczy. Powstawanie wielkich firm wymaga czasu, choć kierunkowo jest bardzo ważne. Po drugie, nie jest wystarczające, aby nazywać polskimi firmami czempionami jedynie kilka przedsiębiorstw, które wyrastają jeszcze z dawnego systemu, są przedstawicielami tzw. starej gospodarki (sektor wydobywczy, energetyczny i finansowy).

W światowych rankingach największych przedsiębiorstw jest bardzo niewiele podmiotów z Polski lub w ogóle ze względu na przyjęte metodyki ich konstrukcji nie może być w nich sklasyfikowana żadna polska firma. W rankingu *Fortune Global 500* w roku 2021 nie sklasyfikowano żadnego polskiego przedsiębiorstwa, a w latach 2020 i 2022 odnotowano jedynie jedno przedsiębiorstwo z naszego kraju, tj. PKN Orlen, który zmieścił się dopiero w piątej, ostatniej setce.

## 3. Czego o budowie potęgi państwa może nas nauczyć historia ekonomii i biznesu?

Studiowanie historii gospodarczej świata wyraźnie dowodzi, że zawsze dochodzenie do siły ekonomicznej państw było związane z – mówiąc współczesnym językiem – proaktywną polityką gospodarczą. Przykładowo, w okresie merkantylizmu, wielkie znaczenie dla rozwoju ówczesnej Anglii miała polityka popierania eksportu dóbr wysoko przetworzonych. W XX w. wielkiego postępu gospodarczego dokonała Korea Południowa, która aktywnie wspierała rozwój przemysłowych konglomeratów[7].

Współcześnie rozwój Chin nie byłby możliwy bez zaangażowania państwa. W każdym z tych trzech przypadków również istniał wystarczający zakres wolności, aby mogli działać przedsiębiorcy, którzy brali na siebie ryzyko uczestnictwa w życiu gospodarczym[8]. Gospodarka ukierunkowywana mądrą polityką państwa współtworzoną przez ludzi biznesu, którzy w takich warunkach odważnie rozwijają swoje przedsiębiorstwa, może rozwijać się szybciej.

---

[6] Wspomina się o tym w *Strategii na rzecz odpowiedzialnego rozwoju…* op.cit. – przypis autora.

[7] Bardzo ciekawe poglądy na ten temat ma słynny heterodoksyjny ekonomista pochodzenia koreańskiego pracujący na Wydziale Ekonomii Uniwersytetu Cambridge, Ha-Joon Chang. Zobacz na przykład wykłady Ha-Joon Changa w ramach cyklu „Economics for People" https://www.youtube.com/watch?v=qaNTRFOkp0Q&list=PLmtuEaMvh-DZbNVIDHA-MTVH0sLb5HP7Pn; zob. też: Ha-Joon Chang, *Economics: The User's Guide*, Penguin Books, London 2014; odnośnie do zmian w Chinach zobacz: H. Chołaj, *Powrót olbrzyma w zglobalizowanym świecie*, OW SGH, Warszawa 2016 – przypis autora.

[8] Książki będące kompilacjami znanych tekstów o wolności, zebrane przez zespół najbliższych współpracowników prof. SGH Leszka Balcerowicza są godnym polecenia wprowadzeniem do tematyki wolności na gruncie ekonomii: *Odkrywając wolność. Przeciw zniewoleniu umysłów*, Wydawnictwo Zysk i S-ka, Poznań 2012; *Odkrywając wolność 2. W obronie rozumu*, Czerwone i Czarne, Warszawa 2022 – przypis autora.

Dla rozwoju gospodarczego duże znaczenia ma stabilny system instytucjonalny[9]. Państwo nieograniczające swojej roli przede wszystkim do zapewnienia bezpieczeństwa, ale dążące do tego, aby zmniejszać niepewność w otoczeniu firm poprzez sprawne sądownictwo gwarantujące m.in. egzekwowalność umów czy ogólnie mówiąc – praworządność. Państwo może, a nawet powinno w kontekście biznesowym nieco złagodzić swoje podejście wynikające z jego roli suwerena wobec obywateli[10]. Naturalnie, jeżeli obywatel jest jednocześnie przedsiębiorcą, to musi on dostosować się do obowiązujących przepisów prawa podatkowego, ale działania aparatu skarbowego nie mogą mieć charakteru opresyjnego, niekiedy wręcz mogącego zniszczyć cały biznes.

Nieodłącznym warunkiem dla rozwoju gospodarczego jest też ukształtowany na danym obszarze system wartości. Granice oddzielające tereny o odmiennych systemach wartości są w zasadzie niemożliwe do ustalenia. Co więcej, w związku z migracjami oraz mobilnością ludności świata, mamy do czynienia z procesem homogenizacji kultur (dla wielu nośnikiem tego procesu są przedsiębiorstwa globalne). Jednocześnie, wiele państw ma charakter multikulturowy, ponieważ w ich granicach współegzystują obok siebie ludzie o nieco innych lub fundamentalnie innych systemach wartości. Biznes funkcjonuje wobec takich złożonych uwarunkowań.

## 4. Jakie są podstawowe elementy procesu strategicznego?

W tak zarysowanym kontekście realiów życia gospodarczego i zaangażowania państwa w tworzenie ram dla dynamicznego rozwoju, znajdujemy połączenie myślenia na szczeblu makroprocesów z bardzo konkretnymi sugestiami dotyczącymi tego, jak efektywnie myśleć o przyszłości, płynącymi ze strony nauk o zarządzaniu. W szczególności wartościowe uwagi na tematy nas interesujące formułuje zarządzanie strategiczne, którego przedmiotem zainteresowań jest funkcjonowanie przedsiębiorstwa w przyszłości.

Należy przypomnieć, że ogólnie w procesie strategicznym możemy wyróżnić cztery fazy: analizę strategiczną, budowanie strategii, wdrażanie strategii i *follow-up*. Proces strategiczny ma w zasadzie analogiczny układ tych samych następujących po sobie faz, niezależnie od charakterystyki podmiotu, którego dotyczy. Inaczej mówiąc, proces strategiczny realizowany zarówno w kontekście przedsiębiorstwa, jak i w kontekście państwa, będzie podobny. Mówiąc bardzo obrazowo, w kroku pierwszym – dokonując analizy strategicznej – próbujemy „mierzyć siły na zamiary", czyli badamy, czym dysponujemy, oraz staramy się zrozumieć, jakie są najważniejsze cechy otoczenia, w którym działamy.

Zasoby wewnętrzne, którymi dysponujemy, mogą mieć materialny lub niematerialny charakter. Na szczeblu przedsiębiorstwa przeanalizujemy, czy posiadamy na przykład nowoczesny park maszynowy, który pozwala w sposób efektywny wytwarzać określone produkty zaspokajające potrzeby klientów. Przykładem zasobu niematerialnego przedsiębiorstwa może być bardzo rozpoznawalny logotyp. Wartość ekonomiczna najbardziej rozpoznawalnych logotypów na świecie osiąga poziom mierzony w setkach miliardów USD. Siła tego niematerialnego zasobu może być nie do pokonania przez konkurencję, stanowiąc bardzo skuteczną barierę w procesach konkurowania. Podobnie na poziomie państwa, zasoby mogą być materialne lub niematerialne. Różnice pomiędzy państwami w tym zakresie są niekiedy bardzo wyraźne.

---

[9] Zob. D. Rodrik, *Jedna ekonomia, wiele recept. Globalizacja, instytucje i wzrost gospodarczy*, Wydawnictwo Krytyka Polityczna, Warszawa 2011, s. 204–244.

[10] Zob. M. Szczaniecki, K. Sójka-Zielińska, *Powszechna teoria państwa i prawa*, Wydawnictwo Wolters Kluwer, Warszawa 2016.

Bardzo ciekawym przykładem pewnej cechy państwa, która może znacznie determinować procesy rozwojowe, jest dostęp do morza. Brak dostępu do morza niektórych krajów, w szczególności jeszcze przed kilkuset laty, w okresie, kiedy transport drogą morską był głównym sposobem przemieszczania się ludzi i towarów na dłuższe odległości, mógł powodować, że państwo miało mniejsze możliwości bogacenia się.

Innym przykładem zasobu, który może na szczeblu państwa decydować o rozwoju społeczno-gospodarczym, jest kapitał intelektualny. W tym kontekście wielu przedsiębiorców z zagranicy podkreśla, że jest to jeden z najważniejszych czynników branych pod uwagę przy decyzji o tym, czy tworzyć i rozwijać przedsiębiorstwa w Polsce. Polacy są narodem wysoko wykształconym, o rozwiniętych umiejętnościach analitycznych, a także z względnie szeroką znajomością języków obcych, głównie języka angielskiego.

Analiza strategiczna, obok refleksji nad posiadanymi zasobami, obejmuje również, jak wcześniej wspomniano, analizę otoczenia. Jakie są kluczowe megatrendy wyznaczające możliwości działania? Jakie następują zmiany w kulturze? Czy społeczeństwo się bogaci, czy ubożeje? Jaka jest dynamika przyrostu naturalnego? Czy dokonują się dalsze postępy na drodze integracji gospodarczej i politycznej krajów w poszczególnych regionach? Jakie są postępy, jeżeli chodzi o nowoczesne technologie?[11] To tylko niektóre z pytań, na które szukamy odpowiedzi. Analiza otoczenia dokonywana jest, jak widzimy, w wielu wymiarach, które najczęściej obejmują następujące kategorie: otoczenie polityczne, ekonomiczne, społeczne, technologiczne, środowiskowe i prawne.

## 5. Dlaczego myślenie o przyszłości i przyjęcie długiego okresu jako horyzontu czasowego analiz jest istotne?

Strategia – jak wcześniej wspomniano – odnosi się do przyszłości. Formułując więc wizję strategiczną na szczeblu państwa, wyobrażamy sobie pewien przyszły obraz kraju. Wizja powinna być konkretna, nie może być niedookreślona. Przykładowo, możemy wymienić przykładowe elementy takiej wizji polegające na tym, że Polska stanie się europejskim liderem, jeżeli chodzi o powstawanie globalnych firm ukierunkowanych na biznesową współpracę z całym światem. W kontekście naszego kraju byłoby to pewne *novum*, mimo wskazania znaczenia polskich firm czempionów w „Strategii na rzecz odpowiedzialnego rozwoju".

Myślenia o przyszłości państwa w kategoriach długiego okresu nie należy się obawiać. Niektórzy krytykują odważnie takie podejście, akcentując, że często strategiczne wizje mają jedynie pewien marzycielski charakter i *de facto* dotyczą celów nierealistycznych, których nie da się zrealizować lub których zrealizowanie jest ekonomicznie nieracjonalne. Oczywiście, może tak być, jeżeli twórcy strategicznych planów nie znają najlepszych praktyk dotyczących ich definiowania lub świadomie je „naginają" lub lekceważą. Niemniej, warto tego rodzaju dyskusje prowadzić w sposób profesjonalny i odpowiedzialnie zaangażowany, ponieważ mogą one mieć kolosalne, pozytywne skutki.

Można sobie zadawać pytanie, skąd optymizm w tym zakresie. Sprawa jest dość oczywista. Polska należy do dużych gospodarek świata, a finanse publiczne państwa są – dokonując pewnego

[11] Ciekawą inspiracją są ukazujące się co kwartał dodatki *Technology Quarterly* do tygodnika „The Economist" zajmujące się nowinkami technologicznymi i ich zastosowaniami w świecie biznesu. Ogólnie rzecz biorąc, analiza otoczenia zmusza przedsiębiorców do – można powiedzieć – interdyscyplinarnego spojrzenia na świat. Aby dobrze zaplanować przyszłość i skutecznie konkurować, ważne jest kompleksowe, analityczne spojrzenie. Chodzi bowiem o to, aby uniknąć poważnych błędów związanych ze strategicznym niedopasowaniem oferty przedsiębiorstwa do obecnego, ale przede wszystkim, do przyszłego rynku – przypis autora.

uproszczenia, ale też nie zaciemniając obrazu takim wnioskiem – względnie zbilansowane. Mimo że stopy procentowe, po jakich Polska pożycza dług na rynku międzynarodowym, są wyższe niż te, które dotyczą długu krajów o największym zaufaniu finansistów, ogólnie należymy do państw o zdrowych finansach publicznych, a także – co warto przypomnieć – do państw o znacznej wielkości.

W takich realiach tworzenie nawet dość śmiałych wizji strategicznych jest realne. Może się wiązać po prostu z pewną racjonalizacją i zmianą priorytetów w zakresie wydatków publicznych. Naturalnie, niełatwe politycznie jest przekonywanie elektoratu, żeby oszczędzać i inwestować, odraczając przy tym bieżącą konsumpcję. Ale nawet przy większych projektach strategicznych ich atrakcyjność może być pociągająca dla mas. Z tym że w żadnym wypadku nie sugeruję, pisząc te słowa, tego, żeby ogół społeczeństwa przy okazji dyskusji o strategii miał podlegać jakimkolwiek manipulacjom. To się może po prostu bardzo wszystkim opłacać.

Myśląc strategicznie, trzeba być kreatywnym, a nie ukierunkowanym na kopiowanie rozwiązań już istniejących. Naśladownictwo strategiczne siłą rzeczy powoduje, że sami skazujemy się na konkurowanie z tymi, którzy już jakiś czas dane podejście do systemu gospodarczego z sukcesami stosują. Naturalnie, ważne jest, aby rozumieć, jakie modele rozwoju gospodarczego przynoszą sukcesy, przy czym inspiracje w tym zakresie należy traktować jako swego rodzaju bazę pod działania, które mają kraj czy przedsiębiorstwo rzeczywiście wyróżniać na tle innych.

## 6. Jakie rezultaty może przynieść zderzenie potencjału zasobów państwa i możliwości tkwiących za granicą?

Mając świadomość tego, jak należy realizować proces strategiczny oraz jakie potencjalne korzyści mogą być związane z odpowiednim podejściem do jego zaprojektowania i zrealizowania w praktyce, bardzo klarowny staje się wniosek, że w szerokim zakresie będziemy mieli do czynienia z zewnętrznym wymiarem analiz strategicznych. Nieuchronnością jest zrozumienie, że w nowoczesnym podejściu akceptujemy założenie, iż cały świat jest areną konkurowania. Biznes działa ponad granicami, a Polska nie jest i nie powinna nigdy być odizolowaną gospodarczą enklawą na mapie świata.

Prowadzone przez nas badania naukowe pokazują, że polscy przedsiębiorcy mają świadomość tego, że wychodzenie na rynki zagraniczne może przynosić ogromne korzyści. Spektakularne sukcesy międzynarodowe polskich przedsiębiorstw są jednak rzadkie. Przedsiębiorcy wskazują na wyzwania związane z koniecznością zaangażowania znacznych środków finansowych w działania ukierunkowane międzynarodowo, na przykład w pozyskanie i utrzymanie kompetentnej kadry pracowników, kadry otwartej na świat, znającej języki obce i specyfikę prowadzenia biznesów w różnych kontekstach kulturowych. Dodatkowo, badania pokazują, iż biznesowi brak jest wsparcia, jeżeli chodzi o budowanie i rozwijanie międzynarodowej sieci kontaktów. Wszyscy rozumieją znaczenie osobistych relacji i *networkingu*, ale działania w tym zakresie są trudne i wymagają wsparcia państwa.

Biznes odnoszący największe sukcesy zawsze jest silnie ukierunkowany międzynarodowo, i to w wielu wymiarach. Nie tylko chodzi tu o to, aby dany produkt bądź usługa były oferowane klientom w bardzo wielu krajach świata. Może to mieć też związek z silnym umiędzynarodowieniem grona kierowniczego i pracowników. Zawsze otwartość na świat i ludzi przynosiła korzyści. Wiele dowodów ponownie dostarcza historia. Polska przeżywała swój największy rozkwit w latach, kiedy była najbardziej otwarta na inne narody i była największą na świecie ostoją tolerancji. Do tego zagadnienia jeszcze w tym tekście się powróci.

Trzeba czerpać z tej tradycji i prowadząc działalność gospodarczą ponad granicami, mieć świadomość specyfiki procesu, ale też potencjalnych szans wynikających z mądrych działań za granicą, które z pewnością dają możliwość zbudowania znaczącej przeciwwagi dla zagrożeń. Nowoczesna analiza strategiczna może pomóc w solidnej identyfikacji tych regionów, krajów czy przemysłów, które mogą być komplementarne dla modeli biznesowych polskich firm. W zasadzie warto sobie uzmysłowić pewną sprawę, otóż tak jak przedsiębiorstwa działają ponad granicami, konkurując na całym świecie, tak samo i państwa mogą w nowy sposób zobaczyć możliwości wynikające ze współpracy. Polskie tradycje tolerancji i szacunku dla różnych narodowości i kultur mogą być w tym zakresie niezwykłym wsparciem.

Docelowy obraz można by wyobrazić sobie – tu nawiązujemy do kształtowania wizji strategicznej Polski – w taki sposób, że polskie przedsiębiorstwa coraz częściej współkształtują światowe łańcuchy dostaw. Klucz do sukcesu tkwi w pewnej zmianie mentalności i spojrzeniu na rzeczywistość jakby z innej, odmiennej perspektywy.

## 7. Jakie narzędzia powinny być używane do prowadzenia analiz strategicznych w czasach globalizacji?

Żyjemy w czasach silnej globalizacji jako procesu, który polega na coraz ściślejszej współpracy gospodarczej pomiędzy krajami. W takich warunkach koniecznością, a może lepiej – przejawem rozsądku – jest zdefiniowanie sensownego wektora polityki mądrej otwartości na świat. Tradycyjne narzędzia wypracowane przez praktyków oraz świat nauki nie wystarczają, aby stale monitorować i rozumieć zmieniający się świat. Wobec powyższych uwarunkowań istnieje – można powiedzieć – wymóg interdyscyplinarności prowadzonych analiz strategicznych, warunek szerokiego spojrzenia na otoczenie.

Znaczenie bardzo profesjonalnego i mającego odpowiednie możliwości działania zaplecza analitycznego dla polskiego biznesu ukierunkowanego międzynarodowo w przedstawianej przez nas perspektywie jest więc zagadnieniem o centralnym, kluczowym znaczeniu. Nie da się odnosić dużych sukcesów na rynkach zagranicznych bez uwzględnienia w działaniach gospodarczych wiedzy o poszczególnych regionach, państwach, rynkach docelowych. Wiedza ta musi być możliwie kompletna, aktualna, ale też dostępna. Ważnym elementem składowym nowoczesnej analizy strategicznej musi być też rzetelna analiza zagrożeń i ryzyk, których w biznesie oczywiście nie da się wyeliminować, ale które należy rozumieć i umiejętnie wobec nich nawigować.

Polska jest krajem, który prowadzi szereg działań ukierunkowanych na wsparcie polskiego biznesu w wymiarze międzynarodowym związanych z gromadzeniem i udostępnianiem wiedzy na temat poszczególnych rynków. Działania też można uznać wstępnie za rozproszone (kilka zaangażowanych instytucji państwowych i organizacji), a także jednocześnie dość skromne, jeżeli chodzi o dostępny budżet, a w konsekwencji – faktyczne oddziaływanie. Pilnym wyzwaniem jest koordynacja wiedzy i działań różnych instytucji i służb państwa.

## 8. Jak należy mądrze wykorzystać unikalne zalety Polaków w budowaniu międzynarodowych relacji?

W naukach społecznych znany jest termin charakter narodowy, który opisuje względnie trwałe właściwości i dyspozycje psychiczne powtarzające się w obrębie danego społeczeństwa oraz ich regularność. Inaczej mówiąc, badacze starają się w ten sposób zrozumieć, jakie przede wszystkich cechy są typowe dla przedstawicieli danej wspólnoty narodowej. Jeżeli chodzi o Polaków, można zaznajomić się z różnymi badaniami w tym zakresie.

Przykładowo, bardzo ciekawe są badania próbujące streścić pewne narodowe wzorce Polaków. Mamy wspaniałą tradycję złotego wieku Jagiellonów, kiedy król Zygmunt August stwierdził, że „nie jest panem ludzkich sumień". Stwierdzenie to oddaje bardzo dobitnie, czym dla Polaków w klasycznym ujęciu jest otwartość i tolerancja. Nie było drugiego takiego kraju na świecie jak Polska w trudnym okresie reformacji i kontrreformacji, nie było na naszych ziemiach wojen religijnych, nie było dyskryminacji jakichkolwiek mniejszości narodowych. Zwróćmy uwagę, że Rzeczpospolita Obojga Narodów była państwem o ponad czterystuletnim okresie trwania, co może wspierać hipotezę o ugruntowaniu się takich cech bardzo silnie w polskiej mentalności[12].

Na kresach Rzeczypospolitej Obojga Narodów żyli przedstawiciele ponad dwudziestu narodowości. Polska była krajem z największą populacją ludności żydowskiej na świecie, która na naszych ziemiach, głównie na kresach, znalazła bezpieczne schronienie i duże swobody. Można powiedzieć, że Polska świadomie urzeczywistniała idee pluralizmu kulturowego, ponieważ wspierało to dążenie do realizacji w praktyce idei dobra wspólnego.

W zasadzie Rzeczpospolita Obojga Narodów była projektem awangardowym, jeżeli chodzi o idee integracji, znacząco wyprzedzała późniejsze przedsięwzięcia o federalistycznym charakterze, takie jak np. Stany Zjednoczone Ameryki Północnej czy też Unia Europejska (sic!).

Być może więc, po trudnym okresie komunizmu, a następnie – po trudnym okresie swoistego zachłyśnięcia się mechanizmami kapitalistycznej gospodarki, wsparcie dla Ukrainy i okazana wobec tragedii wojennej bardzo daleko posunięta solidarność wydają się kolejnym ważnym punktem zwrotnym, doświadczeniem o charakterze w jakimś sensie formacyjnym, w tym znaczeniu, że właśnie wzmacniającym silne strony polskiej mentalności.

Znaczny kapitał intelektualny i społeczny Polaków będzie wspierał rozwój polskich przedsiębiorstw na rynku globalnym oraz będzie ułatwiał budowanie nowego otwarcia we współpracy z każdym państwem na świecie na zasadach długotrwałych relacji, dla których istotne jest dążenie do realizacji obustronnych korzyści.

Prawdziwe i uczciwe budowanie biznesowych sieci relacji (mówiąc językiem zarządzania, tzw. *networking*) może stać się siłą napędową polskiej gospodarki. Również do takich wniosków dochodzimy, realizując projekt Gospostrateg III pt.: „Mazowsze akceleratorem globalnych przedsiębiorstw". Zauważamy wskazywanie przez rozmówców w wywiadach pogłębionych prowadzonych przez zespół badawczy, że dla biznesu kluczowe znaczenie ma budowanie relacji opartych na zaufaniu[13].

## Zakończenie

Przedmiotowy tekst jest próbą wskazania w oparciu o wstępne badania zrealizowane w ramach projektu Gospostrateg III „Mazowsze akceleratorem globalnych przedsiębiorstw", że na szczeblu państwa duże znaczenie mieć może nowa instytucjonalizacja nowoczesnej analizy strategicznej.

---

[12] P. Tarasiewicz, *Specyfika Polaków jako narodu*, „Cywilizacja" 2011, nr 37, s. 40–50.

[13] W ramach projektu Gospostrateg wydano trzy pierwsze publikacje projektowe, z których każda ma znaczenie z punktu widzenia diagnozy sytuacji oraz formułowanych w tym tekście rekomendacji. Zobacz: *Wyzwania związane z globalizowaniem mazowieckich przedsiębiorstw. Eksploracyjne badania diagnostyczne*, praca zbiorowa pod red. H. Rachoń i M. Wojtysiak-Kotlarskiego, OW SGH, Warszawa 2022; *Współpraca w ramach trójkąta relacji administracja–nauka–biznes a wsparcie internacjonalizacji*, praca zbiorowa pod red. E. Pawęty, P. Pietrasieńskiego oraz M. Wojtysiak-Kotlarskiego, OW SGH, Warszawa 2022, a także: *Uwarunkowania ekspansji zagranicznej przedsiębiorstw z województwa mazowieckiego. Analiza regionów światowej gospodarki*, praca zbiorowa pod red. M. Wojtysiak-Kotlarskiego, K. Kacperczyk i A. Domańskiej, OW SGH, Warszawa 2022.

Polsce potrzebna jest w bardziej niż dotychczas kompleksowym ujęciu aktualna, wielowymiarowa i dostępna dla przedsiębiorców wiedza na temat zagranicznych rynków wszystkich państw świata. Analizy te, obok szeregu szans, muszą również obejmować identyfikowanie zagrożeń dotyczących gospodarowania w skali międzynarodowej.

Polska to kraj bogaty, stać nas na bardzo wiele. Skala budżetu państwa daje możliwość realizacji ogromnych projektów modernizujących kraj. Warto myśleć o przyszłości państwa, wykorzystując dotychczasowe doświadczenia w tym zakresie, ale również doskonaląc podejście. Kluczowym czynnikiem sukcesu może być umiejętność budowania przez Polaków w relacjach międzynarodowych kapitału zaufania dzięki rozwijaniu partnerstw opartych na obopólnych korzyściach.

## Literatura


Chang H-J., *Economics: The User's Guide*, Penguin Books, London 2014.

Chołaj H., *Powrót olbrzyma w zglobalizowanym świecie,* OW SGH, Warszawa 2016.

Kołodko G.W., *Świat w matni. Czwarta część trylogii*, Wydawnictwo Prószyński i S-ka, Warszawa 2022.

Leduff Ch., *Detroit. Sekcja zwłok Ameryki*, wyd. 3, Wydawnictwo Czarne, Wołowiec 2019.

*Odkrywając wolność. Przeciw zniewoleniu umysłów*, Wydawnictwo Zysk i S-ka, Poznań 2012.

*Odkrywając wolność 2. W obronie rozumu*, Czerwone i Czarne, Warszawa 2022.

*Polski ład*, https://www.gov.pl/web/polski-lad/o-programie.

Rodrik D., *Jedna ekonomia, wiele recept. Globalizacja, instytucje i wzrost gospodarczy*, Wydawnictwo Krytyka Polityczna, Warszawa 2011.

*Strategia na rzecz odpowiedzialnego rozwoju do roku 2020 (z perspektywą do 2030 r.)*, https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju.

Szczaniecki M., Sójka-Zielińska K., *Powszechna teoria państwa i prawa*, Wydawnictwo Wolters Kluwer, Warszawa 2016.

Szymański W., *Interesy i sprzeczności globalizacji. Wprowadzenie do ekonomii ery globalizacji*, Wydawnictwo DIFIN, Warszawa 2004.

Tarasiewicz P., *Specyfika Polaków jako narodu*, „Cywilizacja" 2011, nr 37.

*Uwarunkowania ekspansji zagranicznej przedsiębiorstw z województwa mazowieckiego. Analiza regionów światowej gospodarki*, praca zbiorowa pod red. M. Wojtysiaka-Kotlarskiego, K. Kacperczyk i A. Domańskiej, OW SGH, Warszawa 2022.

*Współpraca w ramach trójkąta relacji administracja-nauka-biznes a wsparcie internacjonalizacji*, praca zbiorowa pod red. E. Pawęty, P. Pietrasieńskiego oraz M. Wojtysiaka-Kotlarskiego, OW SGH, Warszawa 2022.

Wykłady Ha-Joon Changa z cyklu „Economics for People", https://www.youtube.com/watch?v=qaNTRFOkp0Q&list=PLmtuEaMvhDZbNVIDHA-MTVH0sLb5HP7Pn, www.un.org/ohrlls/sites/www.un.org.ohrlls/files/landlocked_developing_countries_factsheet.pdf.

*Wyzwania związane z globalizowaniem mazowieckich przedsiębiorstw. Eksploracyjne badania diagnostyczne*, praca zbiorowa pod red. H. Rachoń i M. Wojtysiak-Kotlarskiego, OW SGH, Warszawa 2022.

***Beata Wiśnicka***

*Niezależny ekspert. Absolwentka Szkoły Głównej Handlowej w Warszawie. Ukończyła kurs AML na poziomie zaawansowanym w The International Compliance Association w Londynie. Członkini Zarządu w Association of Certified Financial Crime Specialists – Central European Chapter. Pełni funkcję MLRO dla Instytucji Płatniczej. Wdrażała procesy AML i KYC dla klientów z: Polski, Litwy, Łotwy, UK, Cypru, Malty, Gibraltaru, Panamy, Chin, Australii. Od kilku lat związana również ze światem krypotwalut. Swoją wiedzą wspierała także banki w Szwajcarii. Dla firm w procesie uzyskania licencji Krajowej Instytucji Płatniczej projektuje indywidualne rozwiązania AML. Wyszkoliła setki ekspertów AML w Polsce. Pomysłodawczyni kanału Youtube „Jak nie dać się oszukać". Mentorka w programie Perspektywy Women in Tech.*

# Bankowość korespondencka

Bankowość korespondencka pozostaje ważną alternatywą z punktu widzenia wydajności i kosztów, która może być wykorzystywana w przypadku, gdy płatności nie mogą być przetwarzane bezpośrednio przez system płatniczy lub do dokonywania płatności między systemami. W rzeczywistości większość systemów płatniczych obejmuje rynek krajowy (tj. rynek krajowy i rynek strefy euro) oraz niektóre zintegrowane rynki płatnicze, takie jak Jednolity Obszar Płatniczy w Euro.

Ponadto banki międzynarodowe z bezpośrednim dostępem do systemów płatniczych w różnych obszarach walutowych są rzadko spotykane, głównie ze względu na restrykcyjne zasady dostępu do systemów płatniczych, a także koszty zakładania oddziałów i filii w innych krajach, które mogą uzyskać dostęp do systemu płatniczego. Sieć bankowości korespondenckiej może być postrzegana jako ogólnoświatowa sieć relacji dwustronnych, umożliwiająca klientowi banku dokonywanie i otrzymywanie płatności w dowolnej walucie od/do praktycznie każdego kontrahenta posiadającego konto bankowe. W tym celu czasami w jedną płatność może być zaangażowanych kilku korespondentów. Z pewnością jest to rozwiązanie dające satysfakcję zarówno bankom, jak i klientom.

Klienci banku respondenta nie mają bezpośredniego dostępu do rachunku korespondenta, ale prowadzą transakcje pośrednio.

Bankowość korespondencka może obejmować różne usługi, takie jak:

- przelewy międzynarodowe;
- rozliczanie czeków;
- finansowanie handlu;
- pożyczki;
- usługi wymiany walut.

## Procesy AML w relacji korespondenckiej

W relacji bankowości korespondenckiej instytucja korespondentka będzie monitorować transakcje instytucji będącej respondentem w celu wykrycia wszelkich zmian w profilu ryzyka instytucji będącej respondentem lub wdrożenia środków ograniczających ryzyko (tj. nietypową czynność lub transakcję ze strony respondenta lub ewentualne odstępstwa od uzgodnionych warunków ustaleń regulujących stosunek korespondencki). W praktyce, w przypadku wykrycia takich obaw, instytucja korespondentka skontaktuje się z instytucją odpowiadającą, składając wniosek o udzielenie informacji w sprawie dowolnej konkretnej transakcji, co może prowadzić do zażądania dodatkowych informacji na temat konkretnego klienta lub klientów.

Zalecenia FATF wymagają, aby instytucje finansowe identyfikowały, oceniały i rozumiały ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu oraz wdrażały środki przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, które są współmierne do zidentyfikowanego ryzyka.

Wymogi ostrożnościowe i inne wymogi regulacyjne, a także złożoność, liczba i zmiany w systemach sankcji oraz niepewność związana z wzajemnym oddziaływaniem różnych systemów sankcji i ich zastosowaniem do instytucji finansowych również zostały wymienione jako przyczyny ograniczania ryzyka. Regulacje AML/CFT są zatem tylko jednym z wielu czynników wskazanych jako przyczyny zamykania relacji w ramach bankowości korespondenckiej.

Instytucje współpracujące, oceniając ryzyko swojego respondenta, muszą zapewnić, że ocena jest wystarczająco solidna, aby uwzględnić wszystkie istotne czynniki ryzyka. W ten sposób różne poziomy ryzyka nieodłącznego są jasno rozumiane, a odpowiednie kontrole są stosowane do każdego z nich, zapewniając skuteczne zarządzanie tymi ryzykami. W związku z tym zakres, w jakim należy zastosować dodatkowe środki, będzie różny w poszczególnych przypadkach, w zależności od poziomu lub rodzaju ryzyka rezydualnego, w tym środków, które instytucja respondenta wdrożyła w celu ograniczenia własnego ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu.

Czynniki, które należy wziąć pod uwagę przy ocenie ryzyka związanego z bankowością korespondencką, mogą obejmować na przykład jurysdykcję instytucji będącej respondentem, oferowane przez nią produkty/usługi oraz jej bazę klientów. Nie jest możliwe opracowanie ostatecznej listy rodzajów relacji o wyższym ryzyku z kilku powodów. Po pierwsze, nie ma wyczerpującej listy czynników ryzyka, które można by wykorzystać do zidentyfikowania takich relacji, które odnosiłyby się jednakowo do wszystkich relacji. Po drugie, zarówno istotne czynniki ryzyka, jak i odpowiednie środki ograniczające ryzyko muszą być rozpatrywane łącznie, aby stworzyć dokładny i kompleksowy obraz ryzyka.

Nawiązując relację biznesową, w pierwszej kolejności instytucja korespondentka powinna zidentyfikować i zweryfikować tożsamość instytucji respondenta, korzystając z wiarygodnych, niezależnych dokumentów źródłowych, danych lub informacji. Powinna również zidentyfikować i podjąć rozsądne środki w celu zweryfikowania tożsamości beneficjenta rzeczywistego (właścicieli rzeczywistych), tak aby instytucja korespondentka była przekonana, że wie, kim jest beneficjent rzeczywisty instytucji będącej respondentem. W tym celu instytucja korespondentka powinna również rozumieć strukturę własnościową i kontrolną instytucji będącej respondentem. Informacje o strukturze właścicielskiej i kontrolnej obejmują przeprowadzenie weryfikacji pozwalającej instytucji korespondentce nabrać przekonania, że instytucja respondenta nie jest bankiem fikcyjnym. Ponadto instytucja korespondentka powinna zgromadzić wystarczające informacje, aby zrozumieć cel i zamierzony charakter relacji w ramach bankowości korespondenckiej.

Obejmuje to zrozumienie, jakiego rodzaju klientów instytucja będąca respondentem zamierza obsługiwać w ramach relacji bankowości korespondenckiej oraz w jaki sposób będzie oferować usługi, w tym oczekiwanego poziomu działalności, wolumenu i wartości transakcji, charakter planowanych transakcji oraz zakres, w jakim każda z nich została oceniona przez instytucję pozwaną jako obarczona wysokim ryzykiem. Instytucja korespondentka powinna również zgromadzić wystarczające informacje i określić na podstawie publicznie dostępnych informacji reputację instytucji będącej respondentem oraz jakość jej nadzoru, w tym to, czy (i kiedy) była ona przedmiotem dochodzenia w sprawie prania pieniędzy lub finansowania terroryzmu lub działań regulacyjnych.

Ponadto instytucja korespondentka powinna ocenić mechanizmy kontroli AML/CFT instytucji respondenta. W praktyce taka ocena powinna obejmować przegląd systemów i ram kontroli instytucji respondenta w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Ocena powinna obejmować potwierdzenie, że kontrole AML/CFT instytucji będącej respondentem podlegają niezależnemu audytowi (który może być zewnętrzny lub wewnętrzny). Bardziej szczegółowa/dogłębna ocena powinna zostać przeprowadzona w przypadku relacji o wyższym ryzyku, w miarę możliwości obejmując przegląd niezależnego audytu, wywiad z pracownikiem ds. zgodności, przegląd strony trzeciej i potencjalnie wizytę na miejscu.

Instytucja korespondentka powinna również zrozumieć, w jaki sposób instytucja respondenta będzie oferować swoim klientom usługi dostępne w ramach relacji bankowości korespondenckiej, oraz ocenić charakter i poziom ryzyka związanego z rozwiązaniami oferowania. Istnieje kilka możliwych rozwiązań w zakresie oferowania usług.

Relacje w ramach bankowości korespondenckiej są **ze swej natury oparte na wzajemnym zaufaniu** między instytucjami będącymi korespondentami a instytucjami będącymi respondentami, zwłaszcza że instytucje będące respondentami skutecznie wdrażają mechanizmy kontroli AML/CFT. W związku z tym ważne jest, aby instytucje korespondentów utrzymywały stały i otwarty dialog z instytucjami będącymi respondentami, w tym pomagały im w zrozumieniu polityki i oczekiwań korespondentów w zakresie AML/CFT, a w razie potrzeby angażowały się z nimi w celu poprawy ich kontroli w zakresie AML/CFT i procesów. Taka komunikacja wspiera wymóg monitorowania, pomagając oznaczać nowe i pojawiające się ryzyka oraz lepiej rozumieć istniejące, terminowo wyjaśniać wszelkie incydenty, które mogą wystąpić w trakcie relacji biznesowych, wzmacniać środki ograniczające ryzyko i rozwiązywać wszelkie problemy, które mogą powstać w związku z wymianą informacji. Proces ten może również pomóc w budowaniu potencjału instytucji respondentów. Może również pomóc w uniknięciu niepotrzebnych ograniczeń lub zakończenia relacji bez dokładnej oceny ryzyka związanego z konkretnym klientem.

Relacje w ramach bankowości korespondenckiej mają bardzo zróżnicowany charakter i w związku z tym obejmują szeroki zakres wysokich poziomów ryzyka. Poziom i charakter ryzyka mogą się zmieniać w trakcie każdego związku, dlatego w strategii zarządzania ryzykiem odpowiedniej instytucji należy wprowadzić korekty, aby odzwierciedlić te zmiany.

*Anna Krop*

*Analityk kryminalny z kilkunastoletnim doświadczeniem w organach ścigania, trener kompetencji analitycznych.*
*Obiektem jej zainteresowania jest wykorzystywanie nowoczesnych technologii do popełniania przestępstw oraz ukrywania tożsamości.*

# Rzecz w internecie? Czy internet w rzeczy? Przestępczość nowych technologii

## Wstęp

Artykuł podejmuje zagadnienie przestępczości popełnianej przy wykorzystaniu Internetu Rzeczy (IoT)[14], w tym możliwych zagrożeń w obszarze nowych technologii w ujęciu teoretycznym oraz praktycznym. Widoczny jest ścisły związek pomiędzy coraz powszechniejszym korzystaniem z nowoczesnych rozwiązań w komunikacji internetowej a trendami przestępczymi, stanowiącymi wyzwanie zarówno dla bezpośredniego ścigania przestępców, jak i rozpoznawania oraz zapobiegania nadużyciom. Wydaje się on w dużym stopniu niedoceniany w procesie zwalczania przestępczości – zarówno już na etapie szacowania ryzyk jej wystąpienia, jak i w kategoriach źródła wiedzy przy ujawnianiu czynów zabronionych.


[14] Ang. Internet of Things.

Pomimo nadal pojawiającej się opinii, iż przestępczość nowych technologii dotyczy jakiejś bliżej nieokreślonej przyszłości, nie znajduje się ona tam, a otacza nas tu i teraz. Dzieje się tak z powodu boomu technologicznego, którego jesteśmy świadkami i jednocześnie beneficjentami, a który jest niemożliwy do rozpoznania, zrozumienia i opanowania przez pojedynczą osobę, a też często przez całą organizację. Można powiedzieć, że większość planów wychodzenia naprzeciw zagrożeniom IoT z założenia jest zdezaktualizowana, wynika bowiem z reaktywnego procesu rozpoznawania i badania niebezpieczeństw oraz cyklu edukacyjnego, jaki przejść muszą osoby zwalczające przestępczość. Problemu tego nie mają natomiast przestępcy, którzy do zmian adaptują się szybko, korzystając ze wszystkiego, z czego mogą. Zatem każde rozwiązanie, które może wygodnie, szybko i anonimowo doprowadzić ich do celu, jest przez nich wysoce pożądane.

## Internet Rzeczy

Jednym ze sposobów zdefiniowania IoT jest określenie go jako koncepcji połączenia świata wirtualnego i rzeczywistego, opierającego się na trzech filarach, które odnoszą się do cech inteligentnych obiektów. Obiekty te (czyli urządzenia), muszą umieć się wzajemnie rozpoznać, potrafić się ze sobą komunikować i ze sobą współpracować, czyli wzajemnie wpływać na swoje działania. Innymi słowy – Internet Rzeczy oznacza ni mniej ni więcej, że nie tylko ludzie, ale także maszyny i inne urządzenia będą interaktywnie komunikować się przez Internet.

Definiując Internet Rzeczy jako „po prostu punkt w czasie, w którym więcej rzeczy lub przedmiotów było podłączonych do Internetu niż ludzi", firma Cisco Systems oszacowała, że IoT „narodził się" w latach 2008–2009. W latach 2013–2014 szacowano skalę Internetu Rzeczy na 3,8 mld urządzeń, a już w roku 2020 na od 20 nawet do 110 mld urządzeń, przy czym najczęściej oscylowano wokół 20–30 mld. Są to kalkulacje dużych firm informatycznych, naukowców, ale także instytucji państwowych czy unijnych. Z okresu około 2020 r. pochodzą z kolei szacunki dotyczące lat 2025–2030. Wypływa z nich wniosek, że najwyższe prognozy się nie sprawdziły, jednak można obecnie mówić o dużo ponad 20 mld urządzeń.

Gama sprzętów mogących działać w ramach Internetu Rzeczy z każdym dniem się powiększa. Może to być każde urządzenie (lub zbiór urządzeń), które na podstawie danych będzie miało za zadanie wykonać jakieś działanie. Są to zarówno pojedyncze przedmioty (czujniki, żarówki, kamery, zraszacze), mniej lub bardziej złożone systemy (sprzęt RTV i AGD, np. lodówki, pralki czy telewizory, sprzęt badawczy, środki komunikacji), a wreszcie wraz z postępem technologicznym i zwiększoną przepustowością przepływu danych całe domy, osiedla, instytucje oraz miasta.

Sposoby łączności urządzeń IoT będą obejmowały tradycyjną łączność przewodową, jednak w znaczącej większości w ramach Internetu Rzeczy będziemy mieć do czynienia z powszechnie znanymi sposobami transmisji radiowej, w ramach: sieci lokalnej, Wi-Fi, bluetooth, sieci komórkowej (5G), które nie wymagają szczególnego opisywania sposobu działania.

Urządzenia IoT porozumiewają się także powszechnie w standardzie komunikacji, jakim jest ZigBee lub technologiach zbliżonych. Jest to protokół transmisji danych w sieciach bezprzewodowych, który można porównać do Wi-Fi, ale cechuje się on: niższym poborem energii, niewielkimi przepływnościami (do 250 kbps) oraz zasięgiem między węzłami rzędu 100 m. Typowymi zastosowaniami są sieci sensorowe, sieci personalne (WPAN), automatyka domowa, systemy alarmowe, systemy monitoringu. Komunikacja w ZigBee jest dwustronna, co oznacza, że każde urządzenie może odbierać lub wysyłać sygnał, a niektóre nawet przekazywać go dalej. Do jego zalet należy również

natychmiastowy dostęp, dlatego chętnie wykorzystywany jest np. w czujnikach ruchu. ZigBee stworzono z myślą o małej ilości przesyłanych danych i odciążaniu tym samym Wi-Fi. Przy jego użyciu urządzenia raportują zazwyczaj takie informacje, jak poziom baterii czy jakość połączenia, wysyłają sygnał, że coś się dzieje. Nie nadaje się on natomiast do przesyłania dźwięku czy obrazu ze względu na objętość tego typu danych.

## Korzyści, podatności, zagrożenia

W pierwszej kolejności należy zwrócić uwagę na korzyści płynące z utworzenia komunikacji szybkiej (jak 5G) lub niewymagającej wysokich przepustowości (jak ZigBee). Z pewnością jest to rozwój technologiczny, który ma za zadanie polepszenie jakości życia ludzkiego, np.: zwiększenie wygody i komfortu, oszczędność czasu lub energii, ułatwienia w pracy i życiu, wsparcie starszych osób w samodzielności, dbanie o środowisko, optymalizację procesów produkcyjnych czy poprawę bezpieczeństwa.

Jednak prawie każda zmiana lub odkrycie niesie ze sobą nie tylko plusy, ale i minusy. Urządzenia IoT komunikujące się w ramach niskoprzesyłowych technologii danych charakteryzuje ich mały rozmiar, wąskie przeznaczenie, mała pamięć, potrzeba nieobciążania przesyłu danych, chęć oszczędzania energii. Z kolei urządzenia łączące się poprzez 5G są powszechnie umieszczane w miejscach ogólnie dostępnych, niejednokrotnie bez stosowania ograniczeń w dostępności usług. W obliczu tych wszystkich faktów obiekty Internetu Rzeczy narażone są na włamanie, przechwycenie danych, przejęcie zdalne lub fizyczne.

Pierwsze lata rozwoju IoT można porównać do rozwoju samego Internetu – przede wszystkim miał działać. Na etapie jego wykluwania nie martwiono się o bezpieczeństwo tak, jak ma to miejsce teraz. Dlatego specjalnie tworzone dla urządzeń standardy komunikacji typu ZigBee bardzo często nie zapewniają nawet minimum bezpieczeństwa transmisji danych. Nie są one zabezpieczone właściwie lub wcale, np. mają otwarte porty, nie zmienia się w nich ustawień fabrycznych oraz haseł lub w ogóle nie posiadają haseł, transmisja nie jest w żaden sposób szyfrowana. Użyte w urządzeniach karty SIM 5G z kolei bywają niezabezpieczone na poziomie włączonej karty oraz nie mają ograniczeń w zakresie korzystania z usług czy limitów połączeń lub wysyłanych wiadomości.

Potencjał zhakowania i dalszego wykorzystania jest więc ogromny, a ze względu na liczbę i specyfikę urządzeń, nawet dużo większy niż dla samych komputerów. Łatwo sobie wyobrazić, że po uzyskaniu nielegalnej kontroli nad urządzeniem lub siecią jej właściciel, inne osoby i przedsiębiorstwa, instytucje publiczne oraz wszelkie organizacje narażone są na wiele ryzyk. Zaś według szacunków sprzed kilku lat ponad 70% urządzeń IoT zawiera podatności na włamanie.

Wśród zagrożeń płynących z takiego zhakowania wymienić można: dostęp do urządzeń domowych i monitoringu, przejęcie i wykorzystanie danych osobowych, wyłudzenia lub kradzież środków finansowych z podłączonych do urządzeń kart płatniczych czy bezpośrednio kart SIM, szantaże i haracze dotyczące przestojów działalności (np. lodówki podnoszące temperaturę, zablokowanie transportu, paraliż urządzeń do dostarczania przesyłek) lub bezpieczeństwa danych (np. ataki na banki), wykradanie tajemnic przedsiębiorstwa. Kolejnym zagrożeniem mogą być przestępstwa przeciwko zdrowiu i życiu czy też groźby terrorystyczne (np. w sektorze energetyki lub komunikacji zbiorowej). Należy też zwrócić uwagę na zmianę skali i charakterystyki przestępstwa, polegającą na „wejściu do gry" tego rodzaju urządzeń. Oznacza to bowiem pojawianie się nowych możliwości, a zatem modyfikację sposobów działania przestępcy. Inaczej bowiem będzie wyglądało narażenie na utratę

prywatności, gdy stracimy dane z komputera lub ktoś będzie nas podglądał za pomocą jego kamery, a inaczej gdy ktoś zdobędzie dane o naszych preferencjach i zwyczajach w oparciu o oglądane kanały telewizyjne, lokalizacje zapisane na urządzeniach, będzie miał dostęp do kamer monitoringu, elektronicznej niani, a nawet urządzenia sprzątającego czy też jeszcze innych sprzętów domowych.

## Eksperymenty

W ramach zagrożeń IoT przeprowadzono szereg eksperymentów naukowych dotyczących przełamania zabezpieczeń i przejęcia dostępu do urządzeń.

Jeden z nich to spektakularny przykład Jeppa Cherokee, do którego zaplanowano zdalne włamanie i przejęcie kontroli. Po analizie jego wyposażenia znaleziono w systemie rozrywki pokładowej jeden niezamknięty port, co umożliwiło zdalne połączenie się, a następnie uzyskanie dostępu do magistrali CAN, przez którą można było sterować wszystkimi elementami wyposażenia samochodu. Atakujący przejęli kontrolę m.in. nad kierownicą i hamulcami oraz instalacjami użytkowymi (klimatyzacją, wycieraczkami). Pomimo iż kierowca wiedział o eksperymencie, utrata panowania nad pojazdem wywołała u niego szok. W konsekwencji eksperymentu producent samochodu zwrócił się do jego właścicieli z prośbą o kontakt w celu naprawy luki w zabezpieczeniach. Pomimo iż nie doszło do żadnego wypadku, a po zmianach ustawień ataku nie udało się powtórzyć, to fakt, iż był on możliwy, zaniepokoił wszystkich producentów aut. Dotąd łączność z Internetem była reklamowana jako atut, tymczasem zaczęto obawiać się zagrożeń, jakie niesie ze sobą zdalne przejęcie kontroli nad pojazdem. Mogłoby to być np. rozbicie go o przeszkodę, skierowanie na trasę kolizyjną z innym samochodem, potrącenie pieszego czy uwięzienie kierowcy i pasażerów w aucie.

Kolejnym przykładem są dwa eksperymenty dotyczące bezpieczeństwa szpitalnych dozowników leków. Urządzenia te połączone są zazwyczaj z sieciami szpitalnymi, podpiętymi do Internetu i służą do podawania pacjentom leków, których dawki określone są w bibliotekach plików zapisanych w urządzeniu. Oba ataki udało się przeprowadzić dzięki złamaniu zabezpieczeń, po czym: w pierwszym zwiększono dawkę leku w granicach określonych w fabrycznej bibliotece plików, wszelkie zmiany powyżej tej dawki skutkowały alarmem; w drugim zaś udała się podmiana biblioteki plików na zawierające zwiększone dopuszczalne normy leków. To pozwoliło na ustawienie dawki leków na poziomie stwarzającym ryzyko utraty życia przez pacjenta. Ponadto na ekranie dozownika wyświetlały się informacje, jakoby dawka mieściła się w normie. Zidentyfikowaną luką było akceptowanie każdej aktualizacji oprogramowania, dodanej przez dowolną, nieupoważnioną osobę, nie zaś przez osoby posiadające odpowiednie dostępy (jak np. pracownik producenta oprogramowania czy szpitala). W przypadku pacjentów w ciężkim stanie być może nawet by nie podejrzewano, że doszło do morderstwa.

Zagrożenia związane ze sprzętem medycznym dotyczą też np. osobistych pomp insulinowych. Jakiś czas temu jeden z ich producentów poinformował, że produkowane przez niego pompy mogą zostać zhakowane. Komunikacja między pompą a sterującym nią pilotem nie jest bowiem szyfrowana i ktoś obeznany, stojący w odległości kilku metrów od cukrzyka może się do urządzenia podpiąć, a potem zaaplikować choremu dodatkowe dawki insuliny. Można to wykorzystać do szantażu, grożenia śmiercią, a nawet naprawdę do pozbawienia kogoś życia.

## Internet Rzeczy w mediach

Wątki dotyczące zdalnego hakowania urządzeń domowych, medycznych czy pojazdów pojawiają się od wielu lat w kulturze masowej, głównie w filmach i serialach. Jednym z takich przykładów

jest scenariusz drugiego sezonu serialu „Homeland", w którym terroryści w jednym z odcinków zabijają wiceprezydenta USA, wykorzystując jego rozrusznik serca. Urządzenie łączy się za pomocą fal radiowych z programem kontrolującym jego pracę. Terroryści przejmują je i wywołują śmiertelny atak serca polityka. Czy to tylko fantazja hollywoodzkich scenarzystów? Otóż niekoniecznie – w 2007 r. ówczesny wiceprezydent USA Dick Cheney po wszczepieniu rozrusznika postanowił ustalić, czy zagrożenie cyberatakiem jest możliwe. Ponieważ od specjalistów usłyszał, że tak, nakazał wyłączenie możliwości bezprzewodowej łączności z rozrusznikiem. Celem wyposażenia tego typu urządzeń w łączność jest możliwość zdalnego monitorowania przez lekarza stanu pacjenta, a także uratowania życia w sytuacji awaryjnej poprzez wysłanie impulsu przywracającego prawidłową pracę serca. Jednak ze względu na małe rozmiary rozruszników nie posiadają one zabezpieczeń szyfrujących połączenie. Dick Cheney przyznał się do rezygnacji ze zdalnego połączenia dopiero w 2013 r., już po emisji wspomnianego odcinka serialu. Natomiast możliwość zhakowania rozruszników udowodniły eksperymenty na fantomach. Wykazały, że można wpływać na tętno, a w razie wyposażenia rozrusznika w zdalnie aktywowany defibrylator możliwe jest wysłanie komendy, wywołującej kontrolowane wstrząsy elektryczne manipulujące pracą sztucznego serca.

## Podsumowanie

Środowiska hakerskie od lat dyskutują o wykorzystaniu IoT do swoich celów – czyli czerpania korzyści finansowych z ataku na urządzenia podłączone do Internetu. Dla zarobku hakerzy sprzedają dostępy do urządzeń, np.: ruterów, kamer internetowych i drukarek, które można wykorzystać do ataków. Dlatego też mogą sprzedać dostęp do każdego urządzenia lub przygotować je do właściwego ataku.

Natomiast człowiek, wprowadzając do cyberprzestrzeni ogromne ilości informacji oraz przenosząc odpowiedzialność za czynności i procesy na maszyny, żyje wygodniej, jednocześnie narażając się na nowe zagrożenia. Do stworzenia skutecznych zabezpieczeń potrzebny jest czas i praktyka. Jak w prawie każdym przypadku, budowanie bezpieczeństwa polega na pościgu za światem przestępczym i jego metodami działania, a Internet oraz technologie pokrewne zaopatrują przestępców w nowe możliwości działania, obnażając podatność i wrażliwość społeczeństwa informacyjnego.

***dr hab. Kacper Gradoń***

*Wykładowca akademicki, ekspert w dziedzinie kryminalistyki oraz analizy kryminalnej, adiunkt Politechniki Warszawskiej, pracownik naukowy University College w Londynie oraz University of Colorado Boulder*
*Zakład Cyberbezpieczeństwa, Politechnika Warszawska,*
*kacper.gradon@pw.edu.pl*
*Department of Security and Crime Science, University College London,*
*k.gradon@ucl.ac.uk*
*University of Colorado Boulder, Prevention Science Program,*
*kacper.gradon@colorado.edu*

# Dezinformacja a techniki Sztucznej Inteligencji – miecz obosieczny?

Infodemia jest jednym z najbardziej palących problemów współczesnego świata, co przyznają organizacje międzynarodowe – zarówno cywilne, takie jak agencje Organizacji Narodów Zjednoczonych (Światowa Organizacja Zdrowia i UNESCO) czy instytucje Unii Europejskiej (Parlament Europejski, Komisja Europejska), organizacje wojskowe (NATO), jak i policyjne czy wywiadowcze (EUROPOL, Interpol). Infodemia jest pojęciem opisującym przeładowanie informacjami – zarówno prawdziwymi, jak i fałszywymi, które determinują postrzeganie świata przez ich odbiorców, co ma szczególne znaczenie podczas sytuacji kryzysowych o dużym (krajowym,

regionalnym, globalnym) znaczeniu i zasięgu. Pod tym hasłem kryje się kilka podkategorii, a ich zrozumienie i rozróżnienie jest istotne dla tworzenia odpowiednich strategii zapobiegawczych i mitygacyjnych. Dezinformacja (*disinformation*) jest fałszywą informacją, która jest celowo tworzona i rozpowszechniana z wyraźnym zamiarem wyrządzenia szkody; sfabrykowana treść i kryjące się za nią złośliwe intencje są cechami wyróżniającymi dezinformację. Termin misinformacji (*misinformation*) jest często błędnie używany jako synonim dezinformacji, ale chociaż rozpowszechniane w tym przypadku informacje również są fałszywe, to w intencji ich autorów nie mają na celu wyrządzenia szkody, ponieważ osoby dzielące się nimi wierzą, że są one prawdziwe i dokładne. Wreszcie tzw. malinformacja (*malinformation*) to prawdziwa informacja, która jest rozpowszechniana z wyraźnym zamiarem wyrządzenia szkody (np. poprzez ujawnienie wrażliwych, prywatnych danych, które mogą zaszkodzić reputacji konkretnej osoby, przedsiębiorstwa lub instytucji).

Dezinformacja i misinformacja nie są nowymi zjawiskami, jednak ostatnie wydarzenia, takie jak pandemia COVID-19, niesprowokowana agresja militarna Federacji Rosyjskiej przeciwko Ukrainie czy rosnące napięcia związane z roszczeniami terytorialnymi Chińskiej Republiki Ludowej wobec niepodległej Republiki Tajwanu bez wątpienia przyczyniły się do wyraźnego wzrostu natężenia propagacji szkodliwych, fałszywych czy wprowadzających w błąd informacji na poziomie globalnym. Należy podkreślić, że wszelkiego rodzaju sytuacje kryzysowe, w tym katastrofy naturalne, okresy niepokojów i napięć społecznych, wydarzenia polityczne o znaczeniu ponadnarodowym czy istotne zmiany makroekonomiczne stanowią pożywkę dla dezinformacji i mogą stać się narzędziem do prowadzenia operacji informacyjnych, będących elementem szerszych strategii militarnych. Tego rodzaju działania nie są niczym nowym, jednak aktualnie musimy mierzyć się ze znacznie większą skalą takich problemów oraz nieporównanie potężniejszymi możliwościami ich błyskawicznego rozpowszechniania.

Od lat obserwujemy stały wzrost zasięgu i znaczenia mediów elektronicznych, jednak obecnie doświadczamy bezprecedensowych (w skali wielu dziesięcioleci) światowych zagrożeń epidemiologicznych, gospodarczych i militarnych ze wszelkimi ich społecznymi, ekonomicznymi i politycznymi konsekwencjami. Stają się one idealnym podłożem dla tworzenia i rozpowszechniania rozmaitych teorii spiskowych, wzmagają aktywność propagandową szerokiego spektrum ruchów ekstremistycznych i dają idealne możliwości zorganizowanym (sterowanym i kontrolowanym na szczeblu państwowym) kampaniom kategoryzowanym jako elementy wojny informacyjnej (w czym – co szczególnie istotne – specjalizują się, na poziomie państwowym, Federacja Rosyjska i Chińska Republika Ludowa). Media elektroniczne, a przede wszystkim sieci społecznościowe sprzyjają wyjątkowo szybkiej propagacji wszelkiego rodzaju informacji oraz prowadzą do utrwalenia tzw. baniek informacyjnych, czyli sytuacji, w których grupa ludzi posiada ograniczoną wiedzę na temat danego zjawiska, a ich przekonania i poglądy na jego temat są wzajemnie wzmacniane przez towarzyszącą im w danym czasie narrację medialną lub społeczną. W konsekwencji osoby takie przyjmują jako prawdziwe tylko informacje i opinie, które potwierdzają ich wcześniejsze przekonania, a odrzucają te, które nie pasują do ich wizji świata. Bańki informacyjne prowadzą do nieporozumień, uprzedzeń i konfliktów między różnymi grupami ludzi, którzy mają odmienne poglądy na dany temat. Użytkownicy sieci społecznościowych funkcjonujący wewnątrz takich środowisk mają tendencję do ignorowania faktów, które kwestionują ich przekonania, co utrudnia osiągnięcie konsensusu i rozwiązywanie problemów społecznych. Współczesne media społecznościowe, umożliwiając

użytkownikom dostęp do spersonalizowanych treści i sugerując im podobne treści do tych, które już przeglądają, przyczyniają się do zwiększenia znaczenia baniek informacyjnych, które stają się w konsekwencji doskonałym narzędziem do tworzenia, wzmacniania i dalszego rozpowszechniania treści dezinformacyjnych.

Kampanie dezinformacyjne służą przede wszystkim państwom, w których interesie jest podważanie demokratycznych systemów władzy oraz sianie niepokoju i chaosu w społeczeństwach będących celem takich ataków. Pomaga to władzom państw inspirujących i sponsorujących dezinformację w osiągnięciu ich strategicznych, geopolitycznych celów. W przypadku Federacji Rosyjskiej chodzi tu przede wszystkim o praktyczną realizację strategii wojny hybrydowej (tzw. doktryny Gierasimowa) i destabilizację społeczeństw Zachodu; w przypadku Chin motywacją jest pragnienie zdobycia kluczowej roli supermocarstwa światowego i dominacja gospodarcza. Na nieco niższym poziomie kampanie dezinformacyjne służą również grupom ekstremistycznym (zarówno z lewej, jak i prawej strony sceny politycznej), które wykorzystują te metody do pogłębiania polaryzacji i podziałów w społeczeństwie. W istocie jest to korzystne narzędzie pośrednie dla strategii dezinformacyjnych sterowanych na poziomie państwowym (działalność konkurencyjnych ruchów ekstremistycznych w kraju może być podsycana przez wrogie państwo, czego świadkami byliśmy w 2020 r. w Stanach Zjednoczonych, gdzie Federacja Rosyjska symultanicznie inspirowała przeciwne strony konfliktu w okresie poprzedzającym wybory prezydenckie; w opinii instytucji kontrwywiadowczych podobne strategie stosowano już w 2016 r. podczas kampanii wyborczej w USA oraz podczas brytyjskiego referendum związanego z perspektywą wystąpienia Wielkiej Brytanii ze struktur Unii Europejskiej, a także w 2018 r. podczas tzw. protestów „żółtych kamizelek" we Francji).

Z perspektywy instytucji międzynarodowych najpoważniejszym zagrożeniem jest właśnie strategia wojny hybrydowej, gdzie przy użyciu metod dezinformacji steruje się nastrojami społecznymi i manipuluje opinią publiczną, podważając legitymizację organizacji i sojuszy międzynarodowych (Unia Europejska, NATO, WHO). Rozpowszechnianie fałszywych wiadomości ma również bezpośrednie negatywne przełożenie na krajowe i międzynarodowe strategie, czego niedawnym przykładem (podczas pandemii COVID-19) było podważanie powszechnych procedur z zakresu zdrowia publicznego, które destabilizowane były przez stymulowaną przy użyciu technik dezinformacyjnych działalność ruchów antyszczepionkowych. Aktualnie, w czasie rzeczywistym, obserwujemy tego rodzaju zagrożenia w odniesieniu do bieżących konsekwencji wojny na Ukrainie, gdzie Federacja Rosyjska wykorzystuje strategie dezinformacyjne jako ważny element uzupełniający „kinetyczną" stronę konfliktu. Również przestępcy (w tym zorganizowane grupy przestępcze), jak i organizacje terrorystyczne wykorzystują strach, niepokój i niepewność związane z sytuacjami kryzysowymi, intensyfikując działania należące do szerokiej kategorii cyberataków (w tym ataków typu cyber-enabled, gdzie technologie informacyjne służą do przygotowania i przeprowadzenia operacji w świecie rzeczywistym) – kreatywnie przekuwając dotychczasowe metody na takie, które korzystają z okoliczności i skutków społecznych konkretnych typów zagrożeń. I w takich przypadkach mamy do czynienia z wykorzystywaniem technik manipulacyjnych korzystających z metod dających się kategoryzować jako działania dezinformacyjne. Fałszywe wiadomości rozpowszechniane za pośrednictwem mediów elektronicznych (w tym – w szczególności – mediów społecznościowych) stanowią także bardzo poważne zagrożenie dla bezpieczeństwa gospodarczego (na poziomie makroekonomicznym – np. w przypadku podważania zaufania do stabilności strategicznych sektorów gospodarki konkretnego państwa), jak również dla bezpieczeństwa i prowadzenia dzia-

łalności gospodarczej realizowanej przez przedsiębiorców (nieuczciwa konkurencja wykorzystująca metody dezinformacyjne do podważania jakości produktów lub usług oferowanych przez będącą celem ataku firmę). Dezinformacja może również dotykać bezpośrednio konkretnych osób, gdy amplifikowane przy użyciu mediów społecznościowych kampanie oszczerstw mogą przekładać się bezpośrednio na utratę dobrego imienia i idące za tym wymierne szkody osobiste, finansowe czy zawodowe.

Jednym z największych wyzwań, przed którymi stoją krajowe i międzynarodowe instytucje, których zadaniem jest przeciwdziałanie dezinformacji, jest rozwiązanie problemu ogromnych ilość danych, które wymagają analizy. Przepływ informacji, który obejmuje szeroki zakres narracji, zarówno prawdziwych, jak i fałszywych, nie może być analizowany szybko, dokładnie i efektywnie tylko przez wyszkolonych specjalistów, nawet przy wsparciu organizacji zajmujących się weryfikacją faktów. Jakkolwiek należy wspierać i doceniać działalność instytucji i organizacji fact-checkingowych, to należy zauważyć, że ilość danych niezbędnych do przeanalizowania w czasie rzeczywistym i retroaktywnie sprawia, że takie tradycyjne podejście analityczne jest (na poziomie holistycznym i strategicznym) właściwie niemożliwe, a czasem wręcz przeciwskuteczne. Możliwości analizy dużych zbiorów danych, pochodzących z różnego rodzaju mediów (tradycyjnych, elektronicznych i społecznościowych), zbieranych na poziomie międzynarodowym, krajowym, regionalnym i lokalnym i uzupełnionych o dane przestrzenno-czasowe, związane z demografią i mobilnością, muszą opierać się na zastosowaniu odpowiednio skalibrowanych technologii informacyjnych. Z samej natury takich technologii wynika jednak, że mają one cechy „miecza obosiecznego" – tj. ich skuteczność w wykrywaniu dezinformacji sprawia, że po odpowiedniej kalibracji te same narzędzia mogą być wykorzystywane do tworzenia i propagacji szkodliwych i niebezpiecznych treści.

Aktualnie, najistotniejsze praktycznie, zautomatyzowane technologie mające zastosowanie zarówno do tworzenia, jak i wykrywania treści dezinformacyjnych opierają się o algorytmy Sztucznej Inteligencji (Artificial Intelligence – AI) i Uczenia Maszynowego (Machine Learning – ML). Spośród nich szczególne znaczenie w przedmiotowym zakresie mają techniki tzw. Generatywnych Sieci Współzawodniczących (Przeciwwstawnych) – Generative Adversarial Networks (GANs) i Duże Modele Językowe – Large Language Models (LLMs).

Generative Adversarial Networks to modele uczenia maszynowego, składające się z dwóch współzawodniczących sieci neuronowych, zwanych generatorem i dyskryminatorem. GANs są stosowane do generowania nowych próbek danych, takich jak obrazy, dźwięki lub tekst. Generator tworzy próbki danych, a dyskryminator klasyfikuje, czy są one prawdziwe, czy też sztucznie wytworzone. Te dwie sieci neuronowe uczą się wzajemnie i dążą do osiągnięcia równowagi, gdzie generator tworzyć będzie wiarygodne próbki danych, których dyskryminator nie będzie potrafił odróżnić od prawdziwych. GANs są stosowane w wielu dziedzinach, takich jak przetwarzanie obrazów, animacja, syntetyczne generowanie danych i przetwarzanie języka naturalnego. W przypadku dezinformacji możliwe zastosowania GANs obejmują tworzenie fałszywych treści tekstowych (a także grafiki, filmów i dźwięku). W takim przypadku generator może nauczyć się tworzyć fałszywe treści, które wyglądają i brzmią jak prawdziwe, a dyskryminator może nie być w stanie ich wykryć. Z drugiej strony, GANs mogą również pomóc w wykrywaniu dezinformacji. Sieci neuronowe mogą nauczyć się rozpoznawać fałszywe treści, które zostały wygenerowane za pomocą innych GANs, dzięki czemu możliwa jest – teoretycznie – identyfikacja, a następnie usuwanie, flagowanie czy też demaskowanie fałszywych informacji.

Large Language Models (LLMs) to rodzaj algorytmów uczenia maszynowego, które mają zdolność do generowania naturalnie brzmiących tekstów. LLMs są uczone na ogromnych korpusach językowych (tekstowych) i potrafią generować teksty w sposób, który wydaje się naturalny dla odbiorcy. Dzięki temu są w stanie rozumieć kontekst i znaczenie słów, a także odnosić się do istniejącej wiedzy i doświadczeń. LLMs znajdują zastosowanie w wielu dziedzinach, takich jak tłumaczenie maszynowe, generowanie opisów zdjęć, pisanie artykułów i recenzji, a także w tworzeniu chatbotów. Dzięki ich zdolnościom do generowania naturalnie brzmiących tekstów, mogą być wykorzystywane w różnych sytuacjach, gdzie konieczne jest generowanie tekstu na poziomie „ludzkim". Mogą też jednak stanowić zagrożenie, szczególnie w kontekście dezinformacji, gdyż ze względu na swoją zdolność do generowania naturalnie brzmiących tekstów, mogą być wykorzystywane do tworzenia bardzo wiarygodnie brzmiących i napisanych poprawnie językowo fałszywych informacji, które mogą skutecznie wprowadzać odbiorców w błąd. W teorii LLMs mogą również stanowić narzędzie do wykrywania dezinformacji, np. poprzez zaprzęgnięcie tych technologii do rozpoznawania, analizy i klasyfikacji tekstów, jak również do tworzenia rozwiązań służących następnie do weryfikacji faktów. Wykorzystanie LLMs w walce z dezinformacją jest jednak problematyczne, ponieważ modele te mogą zacząć powtarzać i propagować istniejące błędy lub nieprawdziwe informacje, które istniały w dostępnych im danych treningowych.

Obecnie najlepszym i najbardziej aktualnym przykładem zdobywającego popularność rozwiązania opartego o technologie Sztucznej Inteligencji i Uczenia Maszynowego jest ChatGPT. Wykorzystuje on koncepcje Large Language Models (LLM), które zostały starannie przeszkolone na ogromnych zbiorach danych, oraz technologię Generative Pre-trained Transformer 3 (GPT-3). GPT-3 to sieć neuronowa firmy OpenAI oparta na uczeniu maszynowym o pojemności 175 miliardów parametrów, co jest wartością dziesięciokrotnie większą od najbliższego porównywalnego systemu, Turing NLG firmy Microsoft. Potęga modelu OpenAI wynika z zaawansowanego wstępnego szkolenia, a skalę tego procesu dobrze ilustruje fakt, że zasoby Wikipedii stanowią tylko 3% setek miliardów słów wykorzystanych do szkolenia modelu. ChatGPT wykorzystuje technologię uczenia nadzorowanego (Supervised Learning) i uczenia przez wzmocnienie (Reinforcement Learning). Został zaprojektowany jako zaawansowany chatbot, który może obsługiwać wiele różnych zastosowań językowych, a jego główną zaletą jest ogromna szybkość i zdolność do zrozumienia skomplikowanych i zniuansowanych poleceń od użytkownika w wielu językach naturalnych. ChatGPT wyróżnia się dużym zaawansowaniem i szybkością w tworzeniu treści tekstowych, które są przekonujące, logiczne, zgodne z zasadami języka, stylistyki, gramatyki i ortografii. Ma dzięki temu wielki potencjał w zakresie wielu poziomów przestępczego nadużycia technologii. Daje np. możliwość tworzenia bardzo realistycznych i przekonujących wiadomości phishingowych, które są trudne do odróżnienia od prawdziwych i nieszkodliwych komunikatów. Może również służyć do szybkiego i skutecznego tworzenia fałszywych treści o charakterze dezinformacyjnym.

Dostępność tak zaawansowanych technologii, co łatwo może zostać wykorzystane do celów przestępczych i militarnych, stanowi ogromne wyzwanie dla organów ścigania oraz służb wywiadowczych i kontrwywiadowczych. Bezprecedensowa jakość takich narzędzi połączona z ich niskim kosztem, szeroką dostępnością i łatwością użytkowania obniży „próg wejścia" na przestępczy rynek. Dodatkowym problemem jest to, że przestępstwa związane z technologiami sztucznej inteligencji i uczenia maszynowego (takimi jak właśnie ChatGPT) charakteryzują się wysoką skalowalnością,

a ponadto takie techniki mogą być udostępniane, powtarzane lub sprzedawane. Należy również podkreślić rosnące możliwości komercjalizacji technik przestępczych wykorzystujących Sztuczną Inteligencję i Uczenie Maszynowe. Nadużycia AI/ML mieszą się tu w kategorii zagrożeń typu „Crime as a Service" (przestępstwo jako usługa), gdzie kompetentni cyberprzestępcy mogą projektować, oferować i sprzedawać narzędzia informatyczne innym przestępcom, cechującym się ograniczonymi umiejętnościami technicznymi. Dodatkowo, zorganizowane grupy przestępcze, organizacje ekstremistyczne i terrorystyczne lub wrogie państwa, zamiast zatrudniać ludzi do projektowania, pisania i propagowania treści dezinformacyjnych, sami mogą wykorzystać technologie podobne do ChatGPT do tworzenia realistycznych, przekonujących i zróżnicowanych fałszywych i szkodliwych informacji na ogromną skalę i z wielką skutecznością.

Aby skutecznie przeciwdziałać tego rodzaju zagrożeniom, należy dążyć do zbudowania zestawu narzędzi informatycznych (wykorzystujących techniki sztucznej inteligencji, data science i uczenia maszynowego oraz analizy wywiadowczej i analizy semantycznej języka naturalnego), które służyć będą do proaktywnego wykrywania i oznaczania fałszywych informacji w mediach elektronicznych, a także śledzenia ścieżek ich propagacji, identyfikacji punktów węzłowych i dających możliwość ustalenia oryginalnych źródeł dezinformacji. Narzędzia takie (których przykładem mogą być założenia badawczo-wdrożeniowe polskiego projektu Infodemicon) powinny stanowić wsparcie dla agencji rządowych, podmiotów świadczących usługi zdrowotne, mediów informacyjnych, organizacji pozarządowych i sektora prywatnego, pozwalając na zautomatyzowane przetwarzanie i analizowanie informacji w celu wczesnej detekcji potencjalnych zagrożeń. Wykorzystanie narzędzi AI ma potencjał do identyfikacji źródeł dezinformacji, badania sposobu, w jaki dezinformacja przemieszcza się przez sieci i ostatecznie łagodzenia skutków dezinformacji. Przetestowanie tych metodologii możliwe jest w kontekście dezinformacji dotyczącej COVID-19, szczepień przeciw wirusowi SARS-Cov2 oraz w szerokim zakresie w oparciu o dezinformację powiązaną z wojną na Ukrainie. Wiele źródeł dezinformacji jest w tych przypadkach doskonale znanych, co umożliwia walidację technik AI i szkolenie narzędzi AI. Efektem wdrożenia takich rozwiązań powinno być przyczynienie się do zmniejszenia negatywnego wpływu dezinformacji i ograniczenie jej propagacji, co powinno przełożyć się bezpośrednio na ograniczenie możliwości manipulacji opinią publiczną przez grupy przestępcze, organizacje terrorystyczne i ekstremistyczne oraz – przede wszystkim – służby specjalne państw obcych, wrogich naszym wartościom i sojuszom międzynarodowym.

## Literatura:


Calleja N. et al. (incl. K. Gradoń): *A Public Health Research Agenda for Managing Infodemics: Methods and Results of the first WHO infodemiology conference*, in: "JMIR Infodemiology Journal" 2021, Vol. 1, No. 1, DOI: doi:10.2196/30979.

Gradoń K., *COVID-19 and the Information Ecosystem. Lessons from the Russian Malign Influence in the Post-Covid-19 World*, in: *A World Emerging from Pandemic: Implications for Intelligence and National Security* (Eds.: S.E. Pollard and L.A. Kuznar), National Intelligence Press (USA), 2022.

Gradoń K., *Crime in the time of the plague: fake news pandemic and the challenges to law enforcement and intelligence community*, in: "Society Register", 4(2), 133–148, https://doi.org/10.14746/sr.2020.4.2.10.

Gradoń K., *Electric Sheep on the pastures of disinformation and targeted phishing campaigns. The security implications of ChatGPT*, in: IEEE Security & Privacy, Vol. 21 Iss. 3, May-June 2023. DOI: www.doi.org/10.1109/MSEC.2023.3255039, w druku.

Gradoń K., Hołyst J.A., Moy W.R., Sienkiewicz J. i Suchecki K., *Countering Misinformation: A Multidisciplinary Approach*, in: "Big Data & Society" Special Issue on Studying Infodemic at Scale, Vol. 8, Issue 1, May 2021, https://doi.org/10.1177/20539517211013848.

Gradoń K., Moy W.R., *Artificial Intelligence in Hybrid Warfare – a Double-Edged Sword" in: "Artificial intelligence and international conflict in cyberspace* (Eds. F. Cristiano, D. Broeders, F. Delerue, F. Douzet and A. Gery). Routledge, Milton Park (UK), w druku (maj 2023).

Gradoń K., Moy W.R., *COVID-19 Response – Lessons from Secret Intelligence Failures". In: "The International Journal of Intelligence, Security, and Public Affairs*, Vol. 23, Issue 3, 2021, DOI: 10.1080/23800992.2021.1956776.

Moy W.R., Gradoń K., *COVID-19 Effects and Russian Disinformation*, in: "Homeland Security Affairs" 16, Article 8 (December, 2020) www.hsaj.org/articles16533.

***dr hab. nauk prawnych, Wojciech Filipkowski, prof. UwB***

*Kierownik Pracowni Kryminalistyki Zakładu Prawa Karnego i Kryminologii*
*na Wydziale Prawa Uniwersytetu w Białymstoku.*
*Sekretarz naukowy ds. współpracy z państwami zachodnimi*
*Międzynarodowego Centrum Badań i Ekspertyz Kryminologicznych.*
*Autor ponad 160 publikacji naukowych z zakresu prawa karnego,*
*kryminologii i kryminalistyki publikowanych w kraju i za granicą.*

# Propozycja założeń edukacji analityków strategicznych – przyczynek do dyskusji

Strategiczna analiza kryminalna polega na: identyfikacji sposobów dokonywania poszczególnych kategorii przestępstw, ich trendów, szacowanie zagrożeń (*threat assessment*), prawdopodobieństwa ich wystąpienia (*risk assessment*) oraz zewnętrznych względem organizacji czynników, takich jak: zmiany demograficzne, ekonomiczne, społeczne, technologiczne i ich wpływ na przestępczość lub na funkcjonowanie organów ścigania lub służb specjalnych. Definicja tego pojęcia przybliża nas do elementów procesu kształcenia analityka. Proces ten powinien dotyczyć metod i technik prowadzenia analizy oraz czynników mających wpływ na zmiany w dłuższej perspektywie czasowej. Obok celu opisowego i predykcyjnego podkreśla się tutaj także preskryptywny (postulatywny) jej charakter. Właściwe zastosowanie metod i technik prowadzenia analizy prowadzi do wyboru – według kryterium efektywności – rozwiązań prawnych i organizacyjnych, które pozwolą na prawdopodobnie najlepsze przygotowanie się na wyzwania zmieniającej się rzeczywistości.

Strategiczna analiza kryminalna skupia się przede wszystkim na jednej kategorii wyzwań, czyli na przestępczości (lub wybranych kategoriach przestępstw). Są to kategorie pojęciowe oraz przedmioty badań przede wszystkim kryminologii, ale także kryminalistyki oraz prawa. Niniejsza definicja wymienia sposoby dokonywania przestępstw (technika i taktyka kryminalistyczna), trendy w tym zakresie, ale także inne wyzwania, będące czasem zagrożeniami, które mogą mieć potencjalnie negatywny wpływ na funkcjonowanie organizacji, w ramach której przygotowywane są analizy. Wprost wymienione zostały też techniki analityczne, czyli szacowanie zagrożeń oraz szacowanie prawdopodobieństwa ich wystąpienia.

Postawmy sobie pytanie: od czego zależy skuteczność analiz? Jak większość profesjonalnych ludzkich aktywności zależy to od triady czynników: odpowiednio wykształconego i przygotowanego człowieka, opracowanych metodyk postępowania oraz odpowiednio zaawansowanych narzędzi, którymi posługuje się człowiek, realizując metodykę.

Pozwolę sobie wyróżnić 2 grupy cech lub okoliczności związanych z osobą analityka. Są to takie okoliczności, na które nie mamy wpływu, ale nadal są one pożądane i można dobierać kandydatów na analityków według nich, oraz te, na które mamy bezpośredni lub pośredni wpływ. Do pierwszej należą takie cechy osobowości, jak: talent, dobra pamięć, ciekawość, pewność siebie, kreatyw-

ność, otwartość, pracowitość, cierpliwość i wytrwałość oraz pasja. Wynikają one z uwarunkowań np. biopsychologicznych lub wychowania. Druga grupa składa się z 4 podgrup. Po pierwsze, są to umiejętności, które w mniejszym lub większym stopniu można wykształcić lub doskonalić: zdolność do samodzielnej pracy, współpraca w grupie, co powinno być udziałem analityków strategicznych, myślenia analitycznego, sprawnego tworzenia produktów analitycznych, obsługi oprogramowania. Po drugie i trzecie, są to odpowiednio: wykształcenie kierunkowe (z zakresu różnorodnych dyscyplin naukowych) i specjalistyczne. Po czwarte, jest to doświadczenie zawodowe (np. związane z realizacją czynności analitycznych, operacyjno-rozpoznawczych lub dochodzeniowo-śledczych).

Jeżeli chodzi o proces kształcenia, to jako akademik-dydaktyk w swoim imieniu (ale jak sądzę, także Koleżanek i Kolegów naukowców) deklaruję gotowość wsparcia w tym obszarze. Co prawda nie jesteśmy w stanie zapewnić doświadczenia zawodowego analitykom, ale jako akademicy możemy pomóc w jego zbadaniu i naukowym opracowaniu na potrzeby dalszych szkoleń, celem podniesienia ich efektywności.

Jednymi z chyba kluczowych umiejętności po stronie analityka są umiejętności tzw. miękkie. Można nawet pokusić się o stwierdzenie, że niektórzy z nimi się rodzą, a inni muszą sobie je wypracować. Proces kształcenia analityka powinien oczywiście zawierać element selekcyjny, gdzie osoby o już wykształconych kompetencjach powinny znaleźć ich zastosowanie przy wykonywaniu pracy analitycznej. Natomiast po stronie organów ścigania i służb powinno leżeć także stałe podnoszenie tych umiejętności w ramach różnego rodzaju szkoleń specjalistycznych, zawodowych.

Po pierwsze, wydaje się oczywiste, że w przypadku analityków kluczowe znaczenie ma racjonalne podejście do badania i rozwiązywania problemów, które przed nimi zostaną postawione. Wymaga to oczywiście myślenia, nie tylko logicznego (klasycznego), ale także myślenia *out-of-the-box*, czyli kreatywnego, krytycznego podejścia do efektów swojej pracy poprzez kontrolowanie procesu dochodzenia do rozwiązań i samych ich wyników oraz myślenia konstruktywnego, czyli aktywnego poszukiwania jeszcze lepszych rozwiązań tychże problemów. Po drugie, żyjemy w społeczeństwie informacyjnym i jedną z podstawowych współcześnie umiejętności jest poszukiwanie i ewaluacja danych oraz informacji. Ostatnią – moim zdaniem – bardzo ważną umiejętnością jest tzw. zarządzanie sobą w czasie.

Kolejna triada, którą chciałbym przedstawić, dotyczy pracy zespołowej. Biorąc pod uwagę literaturę oraz wyniki badań, można dojść do wniosku, że akurat analiza strategiczna powinna być realizowana w zespołach. Teraz powstaje pytanie: jaki powinien być zoptymalizowany skład takiego zespołu? Ta triada obejmuje trzy kategorie osób według posiadanej wiedzy, umiejętności lub specjalności. Po pierwsze, powinna znaleźć się w nim osoba, która ma wiedzę obszarową na temat problemu. Obejmuje ona wiedzę z wybranych dyscyplin naukowych oraz doświadczenia zawodowego. Po drugie, potrzebujemy osoby, która ma wiedzę o danych funkcjonujących wewnątrz instytucji oraz pochodzących z zewnętrznych źródeł. Po trzecie, potrzebna jest osoba, która ma wiedzę na temat szeroko rozumianych narzędzi, które mogą być wykorzystane do prowadzenia badań lub analiz. Dodam tylko, że osoby te mogą być ekspertami wewnętrznymi, jak również zewnętrznymi. Mogą pochodzić spoza organizacji i będą wtedy pełnić funkcję konsultantów, o ile pozwolą na to uwarunkowania prawne oraz czynniki organizacyjne (np. związane z dostępem do tajemnic państwowych).

Druga grupa problemów dotyczy obszarów, perspektyw czy też dyscyplin naukowych, których to osiągnięcia mogą zostać wykorzystane w ramach prowadzonych badań i analiz strategicznych. Przypomnę koncepcję schematu procesu analizy prof. T. Aleksandrowicza polegającej na poszukiwaniu odpowiedź na pytania: co? i co z tego wynika? Jeżeli zadajemy sobie pytanie co?, to przede

wszystkim pytamy o przeszłość i teraźniejszość: co było? a co jest obecnie? w kontekście badanego przez nas problemu; co pozostaje dla naszej wiedzy ukryte na temat tego problemu?, co powinniśmy jeszcze odkryć? oraz dlaczego tak było i dlaczego tak jest obecnie?, co w przeszłości doprowadziło do stanu obecnego? W kontekście przestępczości jest to podstawowy przedmiot zainteresowania kryminologii w obszarze fenomenologii i etiologii. Kolejnym krokiem jest próba odpowiedzi na pytanie o przyszłość: co będzie? Dlatego też badanie historycznych związków przyczynowo-skutkowych ma ogromne znaczenie. Drugim etapem jest odpowiedź na pytanie, co wynika z tak pozyskanej i zweryfikowanej wiedzy dla funkcjonowania podmiotu, w ramach którego prowadzone są badania? W szczególności dotyczy to konkretnie problemu: jak przygotować go do prawdopodobnie nadchodzących zmian?, jakie środki, którymi dysponuje (albo jeszcze nie, a powinien) będą najbardziej efektywne? Produkt analityczny będzie zawierał propozycje kierunków podejmowanych działań, stanowi wsparcie procesu decyzyjnego.

Do służby w organach ścigania i służbach specjalnych przychodzą ludzie, którzy mają za sobą studia na różnych uczelniach (kierunkach studiów). Optymalnym rozwiązaniem w kontekście naszych rozważań byłoby przyjmowanie osób, które mają odpowiedni zasób wiedzy: związany z metodami badawczymi i technikami analitycznymi lub rozwiązaniami technologicznymi, na temat przestępczości (lub szerzej zagrożeń wymierzonych w państwo lub społeczeństwo). Dlaczego optymalny? Gdyż w takiej sytuacji służba nie musi „tracić czasu" na dokształcanie w kwestiach podstawowych, tylko może przejść do „kształtowania" funkcjonariusza na swoje potrzeby. Poza tym, im bardziej różnorodny pod względem kierunków studiów jest zespół analityczny, tym lepiej, gdyż każdy z jej członków będzie wnosił inną perspektywę na badany problem takiej czy innej przestępczości, inne metody badawcze itd. Ważne jest, że „w sumie" będą się wzajemnie uzupełniać, dając efekt synergii.

Drugi etap to edukacja specjalistyczna. Może ona mieć charakter podstawowy, uniwersalny dla każdej funkcji, jaką funkcjonariusz będzie mógł pełnić w przyszłości w danym podmiocie. Jednak już wtedy można ich zarówno selekcjonować, jak i edukować w wybranych obszarach, co z resztą jest czynione w praktyce (np. kursy analityka kryminalnego). Natomiast edukacja specjalistyczna w stopniu zaawansowanym powinna dotyczyć już wybranych funkcjonariuszy i wysoce wyspecjalizowanych obszarów: technik analitycznych, oprogramowania.

Widzę cztery podstawowe obszary włączenia się uczelni w proces kształcenia analityków strategicznych. Z oczywistych względów uczelnie mają możliwości w postaci zasobów kadrowych do prowadzenia wszelkiego rodzaju procesów kształcenia. Możemy przygotowywać kandydatów do służby w ramach prowadzonych kierunków i przewidzianych *curriculum* specjalności. Możemy też prowadzić lub współprowadzić szkolenia specjalistyczne z wybranych metod badawczych i narzędzi analitycznych lub dzielić się swoją wiedzą obszarową. Ciekawą formą są zamawiane studia podyplomowe, czyli „szyte na miarę" dla konkretnych odbiorców. Daje to szansę kompleksowego i konkretnego zaspokajania potrzeb edukacyjnych organów ścigania i służb specjalnych – w dowolnym miejscu, tzn. na uczelni lub szkołach i ośrodkach szkoleniowych tychże instytucji, ale także w formie *e-learning* (w postaci tzw. *blended learning*).

Natomiast trochę niedocenianym obszarem jest korzystanie z wiedzy eksperckiej pracowników naukowo-dydaktycznych uczelni. Jesteśmy osobami spoza danej instytucji, więc często nie znamy jej specyfiki, jej ograniczeń i możliwości, ale wrodzona lub wyuczona ciekawość, obiektywizm prowadzenia badań każe zadawać nam pytania, porządkować wiedzę, szukać luk i je wypełniać. Znajomość:

zjawisk, rozwiązań obwiązujących za granicą lub dyskursu naukowego pozwala wprowadzić „twórczy ferment" podczas wielu dyskusji. Widzę możliwość współtworzenia kursów szkoleniowych, seminariów tematycznych, opracowywania materiałów szkoleniowych na potrzeby procesu edukacyjnego. Możemy także opiniować istniejące programy szkoleń i sugerować zmiany odpowiadające obecnemu stanowi wiedzy na dany problem w ramach swoich kompetencji naukowych.

Kolejnym obszarem jest prowadzenie badań na potrzeby zamawiającego. Mogą one dotyczyć samego problemu, zjawiska, ale także badania procesu edukacyjnego, rozwijania metod badawczych i analitycznych, naukowego opracowywania dobrych praktyk itp. Podkreślę także znaczenie badań kryminologicznych, kryminalistycznych i prawnych w kontekście przygotowywania i wdrażania rozwiązań technologicznych do praktyki organów ścigania i służb specjalnych służących walce z przestępczością.

Do najważniejszych założeń procesu edukacji analityków strategicznych należy moim zdaniem:

- współpraca interesariuszy w kształceniu podstawowym i specjalistycznym;
- różnorodność w takich obszarach, jak: podmioty szkolące, wykształcenie kierunkowe, skład zespołów analitycznych, źródła danych i informacji;
- produkt analityczny powinien wspierać decydenta w procesie podejmowania decyzji często nieszablonowymi propozycjami, ale też powinien być zgodny z prawdą, a nie jedynie spełniać jego oczekiwania;
- umiejętności „miękkie" są ważne co najmniej w takim samym stopniu jak te „twarde".

## *Jarosław Wolski*

*Polski politolog, dziennikarz, publicysta oraz cywilny analityk OSINT.*
*Od 2014 r. związany z branżą dziennikarstwa obronnego w Polsce,*
*początkowo z portalem Dziennik Zbrojny, a następnie z periodykiem*
*„Dziennik Zbrojny. Analiza", zaś od 2015 r. z „Przeglądem Sił Zbrojnych"*
*oraz jako stały współpracownik (do dziś) z „Nową Techniką Wojskową",*
*(2016) z „Wozami Bojowymi Świata", „FragOut!" (2018).*
*Dziennikarz wydawnictwa Magnum-X („Nowa Technika Wojskowa") oraz*
*„FragOut!" Związany z branżą OSINT.*
*Żonaty od 2011 r., ma syna, zapalony fotograf oraz miłośnik bushcraftu*
*i turystyki industrialnej.*


# „Biały wywiad" (OSINT) – rozwój, rodzaje, możliwości i ograniczenia metody pozyskiwania i analizy informacji pozyskiwanych z jawnych źródeł

Na wstępie należy sobie odpowiedzieć na pytanie „czym jest" OSINT? Najprościej mówiąc jest to biały wywiad oparty o całkowicie jawne i ogólnodostępne źródła. Inaczej rzecz biorąc, można powiedzić, że OSINT jest tak stary jak ludzkość i jej przemieszczanie się w celach kupieckich lub podróżniczych. Zresztą owa podwójna rola handlarzy i podróżników była powszechna i dobrze

znana, zaś ich relacje dotyczące krajów ościennych (choć nie tylko) zawsze stanowiły cenne i uzupełniające źródło informacji. Rewolucja przemysłowa, zdominowanie globu przez Europejczyków oraz następnie rozwój agencji prasowych, korespondentów etc. spowodował że „biały wywiad" stał się powszechny. Wielka wojna, a po niej era totalitaryzmów spowodowały, że taka metoda pozyskiwania informacji – zwłaszcza wobec ZSRR – stała się mniej użyteczna niż w krajach demokratycznych. Totalitarne reżimy stanowiły skrajnie nieprzyjazne środowisko do pozyskiwania wartościowych informacji z jawnych źródeł. Wynikało to z ich braku lub też systemowego fałszowania oficjalnie dostępnych danych. Od produkcji stali, poprzez areały upraw i dzietność małżeństw, po szczepienia ochronne – totalitaryzmy masowo zmieniały dane – albo po to, żeby budować korzystniejszy obraz systemu, albo żeby w ramach systemowej paranoi ukrywać hipotetycznie wrażliwe dane. Niemniej jednak i w czasach dwubiegunowych korzystano z metod OSINT-owych – choć obarczonych bardzo dużym marginesem błędu. „Biały wywiad" powrócił w wielkim stylu wraz z upadkiem dwublokowej rywalizacji i kształtowaniem się multipolarnego ładu światowego, na co nałożyła się z jednej strony globalizacja, a z drugiej strony ewolucja cyfrowa. Rozwój internetu i social mediów spowodował, że OSINT wszedł w swoją złotą erę pod względem łatwości dostępu do danych – zarówno tych ilościowych, jak i jakościowych. W efekcie nastąpiło swoiste „zachłyśnięcie" się „białym wywiadem". Rosyjska agresja na Ukrainę spowodowała, że OSINT wszedł do mass mediów i stał się popularnym określeniem rozpoznawanym nawet przez osoby niezainteresowane tematem, zaś w ramach gwałtownej komercjalizacji jak grzyby po deszczu zaczęły wyrastać różne „kursy" uczące zbierania i obróbki informacji z jawnych źródeł. Czy doprawdy „biały wywiad" we współczesnym wydaniu jest aż tak pożytecznym narzędziem?

Żeby odpowiedzieć na powyższe pytanie, należy sobie zadać pytanie o źródła danych oraz o to, jak dostęp do nich wykształcił dwa zasadnicze rodzaje OSINT-u. Źródła danych są wyjątkowo szerokie, przykładem: social media, gazety, telewizja, periodyki specjalistyczne, systemy logistyczne, kamerki internetowe IP, komercyjne zdjęcia satelitarne, jawne i oficjalne dane rządowe, fora internetowe, wspomnienia młodych emerytów, komercyjne bazy danych etc. Pozorna mnogość źródeł powoduje, że kluczowa staje się ich selekcja i weryfikacja. I tutaj należy przejść do wyjaśnienia różnicy pomiędzy OSINT-em jakościowym a ilościowym.

Ten pierwszy bazuje na wyszukiwaniu i weryfikacji wartościowych informacji dotyczących poszczególnych problemów, np. danego rodzaju sprzętu wojskowego, struktur sił zbrojnych, produkcji zbrojeniowej, wniosków z pola walki itp. Inaczej rzecz biorąc, mówimy w tym przypadku o analizie pewnego wąskiego zagadnienia na podstawie relatywnie małej ilości danych. W efekcie jakość raportów zależy zwykle od doświadczenia i wiedzy analityka, który opracował dane zagadnienie.

OSINT ilościowy bazuje na brutalnej mocy obliczeniowej komputerów oraz na dostępie do możliwie dużej liczby baz danych grupujących dane osobowe, zdjęcia z social mediów itp. Tutaj przeznaczane fundusze mają relatywnie proste przełożenie na jakość raportów. Im zasobniejszy portfel danej organizacji, tym lepsze oprogramowanie działające na BigData oraz więcej dostępnych baz danych. Oczywiście OSINT ilościowy jest zdecydowanie częściej spotykany na poziomie instytucji rządowych, ponieważ w dobie zagrożenia terroryzmem został mocno rozwinięty w oparciu o np. dane z kamer monitoringu miejskiego czy też bazy danych. W efekcie jest on wykorzystywany w zasadzie powszechnie, ale przez „silnych" graczy, czyli służby lub też zasobne firmy międzynarodowe. Jako taki nie będzie jednak stanowić przedmiotu owego artykułu.

Wracając do OSINT-u technicznego – posiada on wiele zalet z punktu wspomagania systemu bezpieczeństwa państwa. Po pierwsze, jest niskokosztowy, o ile zamawiająca instytucja stara się dotrzeć do analityków z pominięciem firm konsultingowych, które zwykle stosują bardzo wysokie narzuty. Na polskim rynku typowa stawka za analizę techniczną dla analityka lub zespołu 2–4 analityków nie przekracza 30 tys. PLN netto. Ich analiza po lekkiej obróbce stylistyczno-graficznej trafia potem na stół jako propozycja firmy konsultingowej w ramach b2g[15] z nieraz dopisanym jednym zerem na końcu jako wyjściowo proponowaną ceną za opracowanie. Po drugie OSINT jest bardzo dobrym spojrzeniem *outside the box*, czyli spoza organizacji. Częstokroć spojrzenie z zewnątrz pozwala na wniesienie wielu interesujących spostrzeżeń, które potem stają się polem weryfikacji przez zamawiającą instytucję. Celem nie jest oczywiście konkurencja lub podważanie pracy instytucji rządowych, ale podwójne sprawdzenie danego zagadnienia z wykorzystaniem innej metody badawczej. Przekłada się to na zwiększenie pewności opracowań, a tym samym bezpieczniejsze diagnozy. Nowoczesny „biały wywiad" jest też bardzo skuteczny zwłaszcza w opisywaniu zagadnień z państw demokratycznych, w których funkcjonują społeczeństwa obywatelskie, w wysokim stopniu sprawdza się też wobec opisywania określonych zagadnień w krajach autorytarnych, w których dyscyplina pilnowania informacji jest przejściowo niska, zaś rozpowszechnienie social mediów bardzo wysokie.

OSINT jakościowy posiada też wymierne ograniczenia, które należy mieć na uwadze podczas korzystania z niego. Po pierwsze jest ograniczony jakością i ilością dostępnych w jawnym obiegu źródeł informacji. Im jest ich więcej i są one jakościowo lepsze, tym trafność raportów jest wyższa. Siłą rzeczy prowadzi to do konkluzji, że najwyższa skuteczność ma miejsce w kwestii raportów dotyczących państw demokratycznych opartych na społeczeństwie obywatelskim i z pluralizmem mediów oraz kulturą pisania jawnych podsumowań, opracowań i raportów. Odwrotna sytuacja ma miejsce w krajach autorytarnych – tutaj przeważnie źródeł jest mało i wymagają owe uważnej weryfikacji. Choć jak pokazuje przykład Rosji i Białorusi, czasami zmiana stylu życia i rozwój social mediów w młodym pokoleniu (millenialsi i generacja Z) znacząco wyprzedzał założenia ochrony informacji niejawnych, które w tych państwach funkcjonowały w zasadzie od rozpadu ZSRR. W efekcie służby obu krajów nie uwzględniały tego, że praktycznie każdy 20-latek ma smartfona z dostępem do internetu i aplikacjami szpiegującymi z funkcją robienia śmiesznych filmików (TikToka) lub social mediami (Facebook, Vk, Instagram), które sprzedają prywatność reklamodawcom. I o ile procedury dotyczące poszczególnych jednostek wojskowych i biur konstrukcyjno-badawczych zwykle były zachowywane, o tyle kończyły się w momencie monitoringu aktywności ich pracowników w social mediach czy też analizy setek filmów z transportów SpW na magistralach kolejowych i drogowych, pomijając oczywiście klasyczną niefrasobliwość poborowych. Dodatkowo utopia retrospektywna za ZSRR części byłych oficerów i inżynierów biur projektowych skutkowała mnogością absolutnie fenomenalnych i jawnych opracowań na temat prac kompleksu wojskowo-przemysłowego z okresu schyłku ZSRR. Fakt, że „nowe" rosyjskie prace badawczo-rozwojowe to w ¾ przypadków dokańczane prace z okresu ZSRR, ułatwiała analitykę mimo autorytarnego charakteru Rosji. I tutaj przechodzimy do drugiego ograniczenia: OSINT jakościowy w dużej mierze bazuje na błędzie czynnika ludzkiego. W przypadku właściwej edukacji społeczeństwa oraz pilnowania procedur w przemyśle i regulaminów w siłach zbrojnych jakość i ilość otrzymywanych

[15] *Business to government* – wymiana między podmiotami gospodarczymi a administracją publiczną.

danych drastycznie spada. Opóźniony jest też czas detekcji danych zjawisk lub zagrożeń. Osobną kwestią – drażliwą dla autorów raportów – jest margines błędu. Sprawdzalność analiz – w zależności od badanego obszaru, a przede wszystkim jakości i ilości dostępnych informacji – wynosi od 60 do 90%. Najpoważniejszym ograniczeniem OSINT-u technicznego jest jednak to, że podlega on gwałtownej i szybkiej redukcji skuteczności w przypadku krajów autorytarnych, które zdiagnozują swoją podatność w tym zakresie. Przykładowo w Rosji od maja lub czerwca 2022 r. rozpoczęto kampanię zamykania lub mocnego cenzurowania for dyskusyjnych na temat obronności, zaczęto też dodatkowo cenzurować rosyjskiego Facebooka (Vk) i zakazano TikToka. Ochrona obiektów kolejowych zaczęła też zwracać baczną uwagę na osoby robiące filmy i zdjęcia. Podjęto również szereg innych działań (przywracanie dyscypliny wykonawczej żołnierzy), w efekcie których ilość informacji dostępnych z social mediów spadła o ponad ¾. Nawet pierwsza fala mobilizacji – cechująca się niską dyscypliną wykonawczą – nie spowodowała znaczącego wzrostu liczby materiałów z zaplecza frontu lub samych działań. Oczywiście zjawiska wyciekania do sieci filmików, jakie robili żołnierze, nie wyeliminowano, ale o rząd wielkości ograniczono częstotliwość występowania zjawiska. Całość przełożyła się na drastyczne pogorszenie ilości i jakości dostępnych informacji.

Mimo powyższych ograniczeń należy uznać, że jednak rola OSINT-u (zarówno jakościowego, jak i ilościowego) będzie nadal rosła na skutek rewolucji w mediach internetowych oraz zmiany stylu życia ludzkości. Będzie to ogólnoświatowy trend, w którym nielicznymi wyjątkami będą państwa totalitarne (Korea Północna) lub reżimy autorytarne (Iran, Rosja, Chiny, Białoruś) zdolne poprzez kontrolę infrastruktury teleinformatycznej (potocznie: dostępu do internetu poprzez punkty węzłowe i lokalnych kontrolowanych przez dany kraj operatorów) oraz restrykcyjne stosowanie drakońskiego prawa wobec własnych obywateli ograniczać skuteczność „białego wywiadu". Niemniej nawet w krajach, takich jak Rosja, Iran czy Chiny nie zdołano całkowicie wyeliminować możliwości OSINT-u, co prowadzi do konkluzji, że wciąż będzie to użyteczne i niskokosztowe narzędzie zbierania oraz opracowywania informacji istotnych z punktu bezpieczeństwa państwa.

Norway grants

CENTRALNE BIURO ANTYKORUPCYJNE CBA

LEAF.2022
law enforcement analysis of the future

Post-conference materials

# Law Enforcement Analysis of the Future

Project "Strengthening of law enforcement agencies and justice system institutions in the area of strategic and operational criminal analysis that will support identification, fight and prevention of corruption and economic crime" funded by Norwegian Financial Mechanism 2014–2021

# Introduction

The international conference LEAF 2022 (Law Enforcement Analysis of the Future), organised by the Central Anti-Corruption Bureau, took place in Warsaw on 26–28 October 2022. The event was carried out in two formats: online and on-site.

Representatives from the law enforcement agencies and academia, as well as independent experts were invited to participate in the event as listeners or speakers.

During the three-day LEAF 2022 conference, crime and strategic analysis specialists, academics, and practitioners presented their lectures. The conference provided an opportunity to discuss and learn about the theoretical perspective on and practice of the issues raised.

During the event, the following lectures were presented:

**26/10/2022**

- – dr hab. Wojciech Filipkowski, Professor of University of Bialystok:
  "Proposed Guidelines for the Education of Strategic Analysts: A Contribution to the Discussion";
- – Beata Wiśnicka-Zawierucha, independent expert:
  "Money Laundering in Correspondent Transactions";
- – Paweł Łukaczyk, National Revenue Administration:
  "Spatial Analysis as Part of Strategic Analysis: The Use in Decision-Making and Law Enforcement Operations";
- – dr hab. Piotr Chlebowicz, Professor of the University of Warmia and Mazury
  "Strategic Criminal Analysis. Implications for the State Security";
- – dr Agnieszka Butor-Keler, Polish Financial Supervision Authority:
  "Anti-Fraud Activities in the Financial Market: Competence and Experience of the PFSA";
- – dr Tomasz Michalak, University of Warsaw:
  "Security Games and their Applications to Defend Critical Infrastructure";
- – Rafał Szczepaniak, Customs and Tax Office in Wrocław:
  "Development of Crime Analysis as Part of the Modernisation of the National Revenue Administration";
- – Karol Drąg, Ministry of Finance:
  "The Importance of Cooperation Between the General Inspector of Financial Information and Law Enforcement Agencies for the Development of Strategic Analysis in the Area of Anti-Money Laundering / Counter Financing of Terrorism"

**27/10/2022**

- – dr hab. Marcin Wojtysiak-Kotlarski, Professor of SGH Warsaw School of Economics: "Modern Strategic Analysis as an Opportunity to Increase Poland's Development";
- – prof. dr hab. Andrzej Zybertowicz: "Clandestine Human Intelligence, the Weaponisation of Economic Interdependence, and Digital Cognitive Degradation: Why the West Failed to Prevent Moscow's Invasion of Ukraine";
- – Radzhami Dzhan, NABU: "Anti-Corruption Authority Analytical Department: Key Points";
- – Tetiana Vodopianova, NABU: "OSINT in Objectives of Freezing, Seizure, and Confiscation of Assets: Challenges and Difficulties";
- – Jarosław Wolski, independent expert: "OSINT as a Tool for Warning of Impending Armed Conflict as a Method for Estimating Losses of Parties to the Conflict";
- – Giovanni Angelini, Guardia di Finanza: "Legal and Regulatory Framework on Assets Freezing Linked to Sanctions to The Russian Federation and Belarus";
- – Roberto Ribaudo, Ministero di Interno:
- "Activity of the Italian ARO / CARIN Office to Implement EU Sanctions. Perspectives on a new European Legal Framework on AROs";
- – dr Tomasz Michalak, University of Warsaw: "AI-Based Solutions for Combating Financial Crime";
- – dr hab. Kacper Gradoń, university lecturer: "Artificial Intelligence in Hybrid Warfare: A Double-Edged Sword"

**28/10/2022**

- – dr inż. Jacek Dajda, AGH University of Krakow: "From Information Analysis to Disinformation: Contemporary Developments in Analytical Solutions Implemented within the AGH Security Centre";
- – dr inż. Fryderyk Darnowski, Central Anti-Corruption Bureau: "From Floppy Disk to Data Lab: Developments in Computer Forensics";
- – dr Harm van Beek, Netherlands Forensic Institute: "Lessons learned from Implementing Digital Forensic as a Service";
- – Joanna Krupa, Central Anti-Corruption Bureau: "Social Trading. Creative Methods of Circumventing the Provisions of the Financial Instruments Trading Act";
- – Dominic Maciver, Gareth Crabbe, National Crime Agency: "International Anti-Corruption Coordination Centre (IACCC) Capabilities to Support Grand Corruption Investigations";
- – Matt Caton, Lee Watkins, National Crime Agency: "Data Exploitation and Biometrics";
- – Anna Krop, crime analyst: "A Thing on the Internet? Or the Internet of Things? New Technology Crimes."


The conference was held as part of the project entitled "Strengthening of law enforcement agencies and justice system institutions in the area of strategic and operational criminal analysis that will support identification, fight and prevention of corruption and economic crime." The project is financed with funds from the Norwegian Financial Mechanism 2014-2021 in the programme area PA20 "International police cooperation and combating crime"' in the "Home Affairs" Programme, allocated through a contest by the Minister of the Interior and Administration.

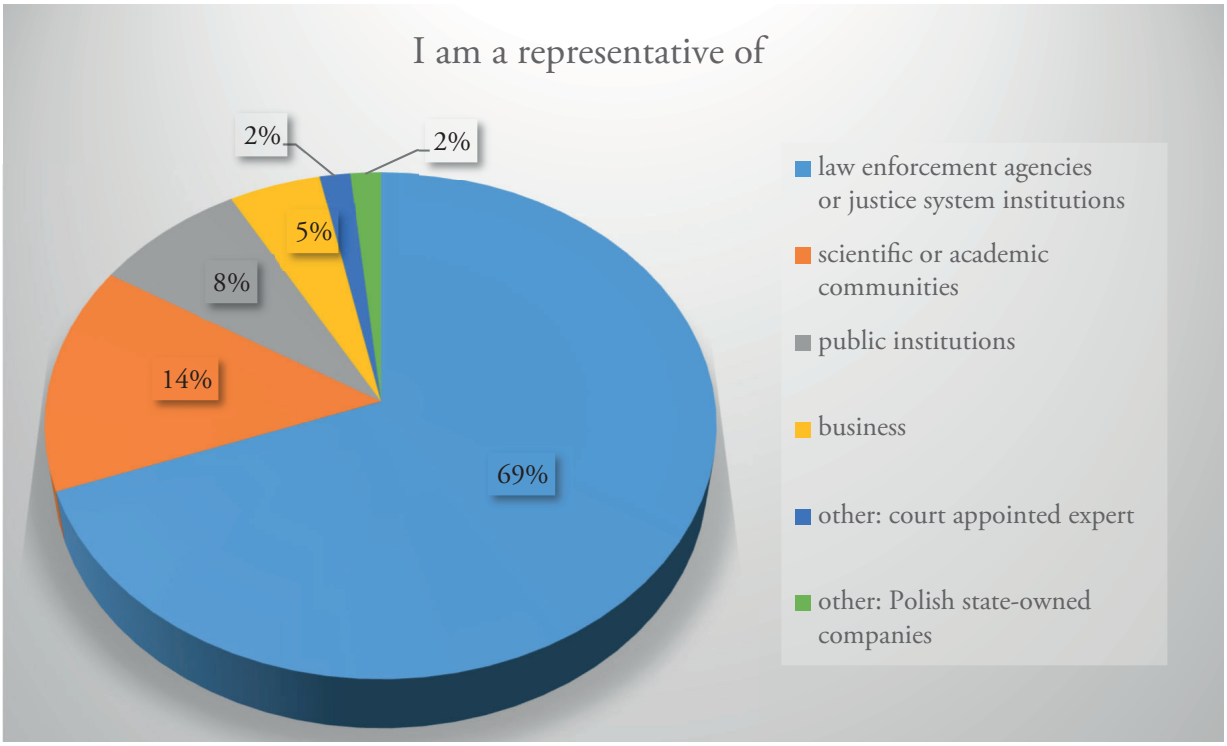
More information on the Norwegian Financial Mechanism and on projects carried out under the Norwegian Funds is available at: www.eeagrants.org / www.norwaygrants.org

www.eog.gov.pl

www.fundusze.mswia.gov.pl.

The conference participants were asked to complete a short anonymous survey to find out their opinions on the event and its possible future. 95 percent of the surveyed conference participants gave the event high and very high ratings; according to the participants, the conference fostered the exchange of knowledge and experience, thus its main objectives were achieved. The selection of topics and speakers were cited as the strongest points of the conference. The participants said in the survey that there should definitely be another edition of the conference including a broader coverage of the topics of forensic analysis and computer forensics.

The structure of conference participants was as follows:




This publication presents articles by the authors who agreed to prepare papers based on their conference lectures.

# Speech by the Deputy Head of the Central Anti-Corruption Bureau opening the LEAF 2022 Criminal and Strategic Analysis Conference

**Dear Participants,**

*I would like to welcome our distinguished guests to an international conference on criminal and strategic analysis. I would also like to extend a warm welcome to our project partners: representatives of the Internal Security Agency, the Military Counterintelligence Service, the National Public Prosecutor's Office, the Ministry of Finance, and our foreign partners: National Anti-Corruption Bureau of Ukraine and the European Union Agency for Law Enforcement Cooperation – Europol.*

*I would like to thank in advance the speakers who decided to share their valuable academic and practical knowledge with us. You contribute to enhancing the analytical capacity of the anti-corruption and economic crime services.*

*I also welcome listeners who have come to us from all over Poland, the United Kingdom, Italy, Portugal, the Czech Republic, Slovakia, Lithuania, Bulgaria, Sweden, and Ireland. Special thanks are due to our Ukrainian guests who, despite the difficult war conditions in their country, decided to come to Warsaw and share their experiences with us.*

*I am glad that you are here with us and hope that this event will contribute to the exchange of ideas and further enhance our cooperation.*

*I also welcome remote conference participants. Thanks to new technologies, despite the physical distance, you can participate in real time in this event, while improving and deepening your skills.*

*I hope that both in-person and remote participants will take away from the lectures what is most important—practical knowledge and inspiration to become ever more effective in detecting and preventing economic and financial crime.*

*The main objective of the project—of which our meeting today is an important part—is to strengthen international cooperation, which is why we decided to invite so many institutions to participate. On many occasions, the handling of the most complex cases in the history of our Bureau would not have been possible without the cooperation of our Polish and foreign partners. With this in mind, I hope that participation in the conference will foster mutual understanding, which will result in even better cooperation in the future. And nothing integrates people like a common goal and working towards it.*

*The threats we face are often cross-border in nature, with greed and the desire to profit at the expense of others often connecting criminals across national borders and time zones. Therefore, I am pleased that to see representatives of the services and law enforcement agencies from so many countries here. What unites us is that we all work to detect and combat serious economic crime that undermines the economic and ultimately the social order of our countries, and therefore, to a large extent, the European order.*

*The fact that we are meeting in the centre of Warsaw and in the centre of Europe is, in a sense, also symbolic. There is a war going on in Europe, just across our border. A war that affects us all in both economic and purely human terms. It is also an information war that is being waged in the media and on the Internet and that actually affects every citizen.*

*Information is a powerful weapon, currency, and one of the world's most valuable commodities. Those who know more win. Information alone, however, does not translate directly into knowledge. This is information that has been processed, integrated and, above all, interpreted in the context of prior knowledge. I hope that everything you, as participants in this conference, will hear and learn will result in the concrete knowledge of how to systematise and interpret information in such a way as to make the fullest and most appropriate use of it. We aim to turn information into knowledge and not just a vast collection of chaotic facts.*

*The lecture topics were also in this aspect. We will address issues of financial and economic analysis in the broadest sense, advanced forensic techniques, new technologies in the service of criminal and strategic analysis, as well as the current geopolitical situation, but still in the context of the tasks facing analysts and law enforcement agencies.*

*In their daily work, the analysts of the law enforcement and intelligence services face complex issues. The most repeated argument for their continuing education is to always be able to stay one step ahead of criminals and therefore use methods and tools that will be effective and efficient. This is the only way we will have a level playing field against our opponents. The methods used by criminals both to commit criminal acts and to cover their tracks, as well as to legalise the funds derived from them are constantly evolving. As services, we should always be at least one step ahead of them in order to not only detect, but also to some extent anticipate and prevent some of those crimes. Strategic and crime analysis is a tool ideally suited to these purposes. It provides the services with the methods and means to systematically and precisely identify threat areas, investigate them for irregularities, and determine further operational and intelligence directions. And that is the primary purpose of this conference: to seek methods to face new challenges effectively and fearlessly, and to promote best practices and solutions in crime and strategic analysis.*

*It is my firm belief that the best solutions are born at the interface between practice and academic knowledge, and therefore, I very much appreciate the participation of the scientific community in this conference and would like to especially thank the academics, the honourable professors, for their presence. Your willingness to share your knowledge is indeed an eminently pro-state activity.*

*I encourage you to actively participate in all three days of the event, as each will have a different focus and leading theme but will undoubtedly complement each other.*

*The in-person participants are also invited to attend a gala dinner to that will be held in the historic fortress, an interesting point on the map of Warsaw's history. Let this evening meeting be an opportunity to exchange opinions and make contacts that will facilitate our further cooperation.*

Daniel Karpeta
Deputy Head of the
Central Anti-Corruption Bureau

***Dr hab. Marcin Wojtysiak-Kotlarski,***

*Professor of SGH Warsaw School of Economics*
*Head of the International Strategies Unit*
*Institute of Management*
*Collegium of Management and Finance*
*SGH Warsaw School of Economics*
*ORCID: 0000-0002-2500-7191*

# "Modern Strategic Analysis as an Opportunity to Increase Poland's Development – a synthetic presentation of the main theses of the author's speech at the LEAF 2022 conference"[16]

## Introduction

Poland is a country whose history, including the economic history, is particularly close to our hearts because it is here that we were born, here that we live, here that we work, here that we raise our children, and so on. Although the modern world is becoming more and more integrated as the process of globalisation, which is a multidimensional mechanism influencing people's everyday actions and activities, is progressing dynamically, the perspective of the well-being of a country's citizens is very important[17].

Despite the numerous organisations that integrate countries, whether politically, economically, culturally or otherwise, individual countries still compete. In turn, the wide accessibility of people in practically every corner of the globe, including, of course, Poland, to knowledge and information on the socio-economic situation around the world, gives rise to new responsibilities, so to speak.

---

[16] This article is inspired by research carried out at the SGH Warsaw School of Economics as part of the project "Mazovia as an accelerator of global businesses." It is a project funded by the National Centre for Research and Development as part of the strategic research and development programme "Social and economic development of Poland under conditions of the globalising markets" GOSPOSTRATEG. The main objective of the GOSPOSTRATEG programme is to increase the use of the results of socio-economic research in shaping national and regional development policies by 2028. The article also draws heavily on the author's presentation at the LEAF 2022 International Conference (Law Enforcement Analysis of the Future) held on 26-28 October 2022, where experts from different regions of Poland and Europe, academics, representatives of intelligence services and independent experts, among others, undertook discussions on strategic analysis conducted in the context of the state. An expanded version of the article was published in: M. Wojtysiak-Kotlarski, *Nowoczesna analiza strategiczna jako szansa na zwiększenie dynamiki rozwoju Polski* [*Modern Strategic Analysis as an Opportunity to Increase Poland's Development*], in: *30 lat w naukach społecznych. Nowe myśli i idee* [*30 Years in Social Sciences. New Thoughts and Ideas*], Oficyna Wydawnicza Szkoły Główna Handlowej w Warszawie, Warsaw 2023, pp. 541-560. This material is in an abridged form of the article indicated above and is primarily intended to present the main theses of the LEAF conference speech – the author's footnote.

[17] See in more detail: W. Szymański, *Interesy i sprzeczności globalizacji. Wprowadzenie do ekonomii ery globalizacji* [*Interests and Contradictions of Globalisation: Introduction to Economics of the Globalization Era*], Wydawnictwo DIFIN, Warsaw 2004.

When we know that a country is hit by a massive famine or a tragic earthquake, we react and help. In such an outlined context, despite the numerous international interdependencies, the criterion of economic policy effectiveness at the local aspect, i.e. at the level of a country's economy, is still very important and relevant.

This article is intended to contribute to the discussion on what is important to make the Polish economy more dynamic. We aim to make development sustainable in economic, social, and environmental dimensions[18]. It should not be the case, for example, that the very strong drive for industrialisation will be pursued at the expense of citizens' health or at the expense of the environment. This article is by no means intended to be comprehensive. It is not possible to cover all the important threads in a short article. Nevertheless, it is the author's intention to share with a wider audience some preliminary insights relating to the research conducted and to contribute with this article to the discussion on how to carry out strategic analysis at the state level in a modern way.

## 1. Strategy building at the state level: essence and some of the challenges

Reflecting on development strategy is a difficult issue but one of extraordinary importance. The strategy sets direction, speaks of priorities, and answers fundamental questions about the future of the state[19]. When we think strategically, we are therefore defining a certain plan on how we want to achieve those goals we set for ourselves in the future.

When formulating a strategy at the state level, it is important to bear in mind that the economy, by definition, operates in the face of the problem of scarcity, which means that it is necessary to accept that it is not possible to achieve everything in the economy that stakeholders expect. It is therefore impossible to overlook the issue of accountability. It is easy to spend taxpayers' or the state's creditors' money. The trick is to do it in an economically rational way.

In the context of the Polish economy, strategies concerning the economy have been defined many times. An element of these strategies has always been a certain vision, i.e. a target image of the state that we want to achieve through the implementation of a given strategy (plan). The strategy contains defined objectives: sometimes there are few, sometimes many. Sometimes they are ambitious and attractive, practice varies. Sometimes they are vague, sometimes difficult to quantify. It is important that they are attractive to the public, ambitious, and feasible.

## 2. Corporate strength as a determinant of economic strength

Charlie Wilson, president of General Motors, uttered the eternal words: "What's good for our country is good for General Motors. And what's good for General Motors is good for America.[20]" Of course, the above statement is somewhat of a simplification. For example, the benefits associated with the operation of a given company are distributed differently among particular stakeholder groups; moreover, even within a given stakeholder group, e.g. managers or employees, there can sometimes be very large spreads in salaries and additional benefits for the same positions.

---

[18] Cf. G.W. Kołodko, *Świat w matni. Czwarta część trylogii* [*The World in a Quagmire. The Fourth Part of the Trilogy*], Wydawnictwo Prószyński i S-ka, Warsaw 2022.

[19] See *Strategy for Responsible Development by 2020 (with an outlook by 2030)* https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju, cf. "Polish Deal" https://www.gov.pl/web/polski-lad/o-programie

[20] See: Ch. Leduff, *Detroit: An American Autopsy* [*Detroit. Sekcja zwłok Ameryki*], 3rd edition, Wydawnictwo Czarne, Wołowiec 2019; cited acc. to: www.polityka.pl, published on 3 March 2015.

Generally speaking, however, there is a fairly widespread view that Poland has enormous economic potential. Poland is currently the nineteenth largest economy according to data published in the *World Economic Outlook Database* by the International Monetary Fund in October 2020. From this point of view, the Polish aspirations to co-shape global economic policy are justified.

After the rather chaotic ownership changes during the transformation period, when privatisation of national assets was in many cases carried out in an overly hasty manner, with insufficient safeguards for the interests of the Polish state, there has been a clearly discernible positive trend in recent years towards emphasising the importance of champion companies being established in the Polish economy[21].

There are two comments to be made on this situation. Firstly, it is not simple to fundamentally remodel an economic system in the short term. The formation of great companies takes time, although directionally it is very important. Secondly, it is not enough to apply the name of call Polish champion companies to only a few enterprises that still grow out of the old system and are representatives of the so-called old economy (mining, energy, and financial sectors).

In the world rankings of the largest companies, there are very few entities from Poland or no Polish company can be classified at all due to the methodologies adopted for their incorporation. No Polish company was ranked in the *Fortune Global 500* in 2021 and only one company from our country was recorded in 2020 and 2022, i.e. PKN Orlen, which only fit into last five hundred entries.

## 3. What can the history of business and economy teach us about building state power?

A study of the economic history of the world clearly demonstrates that the attainment of economic strength by states has always been related with—to put it in modern language—proactive economic policies. During the mercantilist period, for example, the policy of supporting the export of highly processed goods was of great importance to the development of England at the time. In the 20th century, great economic progress was made by South Korea which actively supported the development of industrial conglomerates[22].

Today, China's development would not be possible without state involvement. In each of these three cases, too, there was sufficient freedom of operations for entrepreneurs who took on the risk of participating in economic life[23]. An economy guided by wise state policies co-created by business people who courageously develop their enterprises under such conditions can grow faster.

---

[21] This is mentioned in the *Strategy for Responsible Development*…op.cit. – the author's footnote.

[22] A famous heterodox economist of Korean descent working in the Faculty of Economics at the University of Cambridge, Ha-Joon Chang, has some very interesting views on this subject. See, for example, Ha-Joon Chang's lectures in the series Economics for People https://www.youtube.com/watch?v=qaNTRFOkp0Q&list=PLmtuEaMvhDZbNVIDHA-MTVH0sLb5HP7Pn; see also: Ha-Joon Chang, *Economics: The User's Guide*, Penguin Books, London 2014; for developments in China, see: H. Chołaj, *Powrót olbrzyma w zglobalizowanym świecie* [*Return of the Giant in a Globalised World*], OW SGH, Warsaw 2016 – the author's footnote.

[23] The books compiling well-known papers on freedom collected by a team of SGH Professor Leszek Balcerowicz's closest collaborators, are a worthwhile introduction to the subject of freedom on the ground of economics: *Odkrywając wolność. Przeciw zniewoleniu umysłów* [*Discovering Freedom: Against the Enslavement of Minds*], Wydawnictwo Zysk i S-ka, Poznań 2012; *Odkrywając wolność 2. W obronie rozumu* [*Discovering Freedom 2: In Defence of Reason*], Czerwone i Czarne, Warsaw 2022 – the author's footnote.

A stable institutional system is important for economic development[24]. A state that does not limit its role primarily to providing security but seeks to reduce uncertainty in the corporate environment through an efficient judiciary that guarantees, among other things, the enforceability of contracts and agreements or the rule of law in general. The state can and even should, in the business context, somewhat moderate its approach resulting from its role as sovereign vis-à-vis its citizens[25]. Naturally, if a citizen is also an entrepreneur, they must comply with the applicable tax laws but the actions of the fiscal apparatus must not be of an oppressive nature, sometimes even capable of destroying the entire business.

The value system formed in the area is also an inherent condition for economic development. Boundaries separating areas with different value systems are in principle impossible to establish. Moreover, due to migration and the mobility of the world's population, we encounter the process of homogenisation of cultures (for many, the vehicle for this process is global companies). At the same time, many countries are multicultural because people with slightly different or fundamentally different value systems coexist side by side within their borders. Business operates in the face of such complex conditions.

## 4. What are the basic elements of the strategic process?

In this outlined context of the realities of economic life and the state's involvement in creating a framework for dynamic development, we find a combination of thinking at the level of macro-processes with very specific suggestions on how to think effectively about the future coming from the management sciences. In particular, strategic management, which is concerned with how an enterprise will operate in the future, makes valuable comments on topics that are of interest to us.

It should be noted that, in general, we can distinguish four phases in the strategic process: strategic analysis, strategy building, strategy implementation, and follow-up. The strategic process has an essentially analogous pattern of the same successive phases, regardless of the characteristics of the entity involved. In other words, both the strategic process implemented in the context of the company and in the context of the state will be similar. To put it very figuratively, in step one—carrying out a strategic analysis—we try to "look before we leap," i.e. we examine what we have at our disposal and try to understand what are the most important features of the environment in which we operate.

The internal resources at our disposal may be tangible or intangible in nature. At company level, we will analyse whether we have, for example, modern machinery that allows us to efficiently produce specific products that meet customer needs. An example of a company's intangible asset could be a highly recognisable logo. The economic value of the world's most recognisable logos reaches levels measured in the hundreds of billions of American dollars. The power of this intangible resource can be unbeatable by the competition, acting as a very effective barrier in the competitive processes. Similarly, at the state level, resources can be tangible or intangible. The differences between states in this respect are sometimes very pronounced.

A very interesting example of a certain feature of a state that can significantly determine development processes is access to the sea. The lack of access to the sea for some countries, particularly as recently as a few hundred years ago when transport by sea was the main means of moving people and goods over long distances, may have resulted in the state having fewer opportunities to become rich.

---

[24] See D. Rodrik, *One Economics, Many Recipes: Globalization, Institutions, and Economic Growth* [*Jedna ekonomia, wiele recept. Globalizacja, instytucje i wzrost gospodarczy*], Wydawnictwo Krytyka Polityczna, Warsaw 2011, pp. 204-244.

[25] See M. Szczaniecki, K. Sójka-Zielińska, *Powszechna teoria państwa i prawa* [*Universal Theory of State and Law*], Wydawnictwo Wolters Kluwer, Warsaw 2016.

Another example of a resource that can, at the state level, determine socio-economic development is intellectual capital. In this context, many entrepreneurs from abroad emphasise that this is one of the most important factors taken into account when deciding whether to establish and develop businesses in Poland. Poles are a highly educated nation with well-developed analytical skills and a relatively broad knowledge of foreign languages, mainly English

Strategic analysis, in addition to reflecting on the resources at hand, also includes, as mentioned earlier, an analysis of the environment. What are the key megatrends setting the stage for action? What cultural changes are taking place? Is society getting richer or poorer? What are the dynamics of the birth rate? Is further progress being made towards the economic and political integration of countries in the regions? What progress has been made in terms of modern technologies?[26] These are just some of the questions we are seeking answers to. As we see, the analysis of the environment is carried out in many dimensions that most often include the following categories: political, economic, social, technological, ecological, and legal environment.

## 5. Why is thinking about the future and adopting the long term as the time horizon for analysis important?

Strategy, as mentioned earlier, refers to the future. Therefore, when formulating a strategic vision at the state level, we imagine a certain future picture of the country. The vision should be concrete, it must not be vague. For example, we can mention exemplary elements of such a vision of Poland becoming a European leader in terms of the emergence of global companies focused on business cooperation with the whole world. In the context of our country, this would be something of a novelty, despite the indication of the importance of Polish champion companies in the *Strategy for Responsible Development*.

We must not fear long-term thinking about the state's future. Some have boldly criticised this approach, stressing that often strategic visions have only a certain dreamlike character and *de facto* concern unrealistic goals that cannot be achieved or are economically unreasonable to achieve. Of course, this may be the case if the creators of strategic plans are not aware of best practices for defining them or deliberately "bend" or disregard them. Nevertheless, it is worth having these kinds of discussions in a professional and responsibly engaged manner, as they can have massive positive effects.

One may ask where the optimism in this regard comes from. The case is quite clear. Poland is one of the world's large economies and the state's public finances are—to simplify somewhat but also not to obscure the picture with such a conclusion—relatively balanced. Despite the fact that the interest rates at which Poland creates debt on the international market are higher than those for the debt of the countries with the greatest confidence of financiers, we are generally one of the countries with sound public finances and, as is worth remembering, of considerable size.

In such circumstances, creating even quite bold strategic visions is feasible. It may simply involve some rationalisation and reprioritisation of public spending. Naturally, it is not easy politically to convince the electorate to save and invest while deferring current consumption. But even with

[26] The quarterly *Technology Quarterly* reports published by *The Economist* that focus on technological innovations and their applications in the business world are an interesting inspiration. In general, the analysis of the environment forces entrepreneurs to, one could say, take an interdisciplinary view of the world. To plan well for the future and compete effectively, a comprehensive and analytical view is important. This is because the idea is to avoid serious mistakes related to the strategic mismatch between the company's offer and the current, but above all, future market – the author's footnote.

larger strategic projects, their appeal can be appealing to the masses. Except that I am in no way suggesting by writing these words that the general public should be subject to any kind of manipulation when discussing strategy. It might just be very profitable for everyone.

When thinking strategically, one needs to be creative, not geared towards copying solutions that already exist. Strategic imitation necessarily results in us condemning ourselves to compete with those who have already been successfully applying a given approach to the economic system for some time. Naturally, it is important to understand which models of economic development are successful but inspiration in this respect should be seen as a kind of basis for measures that are intended to make a country or enterprise really stand out from others.

## 6. What results can come from a clash between the potential of the state's resources and the opportunities abroad?

With an understanding of how the strategic process should be implemented and the potential benefits that can be associated with the right approach to its design and implementation in practice, it becomes very clear that we will be dealing extensively with the external dimension of strategic analyses. It is inevitable to understand that in the modern approach we accept the assumption that the whole world is a competitive arena. Business operates across borders and Poland is not and should never be an isolated economic enclave on the world map.

Our research shows that Polish entrepreneurs are aware that reaching out to foreign markets can bring huge benefits. However, spectacular international successes of Polish companies are rare. Entrepreneurs point to the challenges of having to commit significant financial resources to internationally-oriented activities, for example in attracting and retaining a competent workforce that is open to the world and familiar with foreign languages and the specificities of doing business in different cultural contexts. In addition, research shows that business lacks support when it comes to building and developing international contact networks. Everyone understands the importance of personal relationships and networking but actions in this area are difficult and require state support.

The most successful businesses are always strongly internationally oriented, in many dimensions. It is not just a question of a product or service being offered to customers and clients in a great many countries around the world. This may also have to do with the strong internationalisation of the management team and employees. It has always been beneficial to be open to the world and people, to which much evidence is again provided by history. Poland had its greatest heyday in the years when it was most open to other nations and was the world's greatest refuge of tolerance. This issue will be returned to later in this article.

It is important to draw on this tradition and, when doing business across borders, to be aware of the specifics of the process but also of the potential opportunities arising from wise actions abroad, which certainly offer the possibility of building a significant counterbalance to the threats. A modern strategic analysis can help to robustly identify the regions, countries or industries that may be complementary to the business models of Polish companies. In fact, it is worth realising one thing: just as companies operate across borders competing around the world, the same way states can have a new perspective on the opportunities arising from cooperation. Poland's traditions of tolerance and respect for different nationalities and cultures can provide extraordinary support in this regard.

The target picture could be envisaged—here we refer to the shaping of Poland's strategic vision—in such a way that Polish companies increasingly co-shape global supply chains. The key to success lies in a certain change of mentality and looking at reality as if from a different and distinct perspective.

## 7. What tools should be used to carry out strategic analysis in the times of globalisation?

We live in a time of strong globalisation as a process that involves ever closer economic cooperation between countries. Under such conditions, it is a necessity, or perhaps better, common sense, to define a sensible policy vector of wise openness to the world. The traditional tools developed by practitioners and the world of science are not enough to continuously monitor and understand the changing world. In view of the above conditions, there is, one could say, a requirement for interdisciplinarity in the strategic analyses, a condition for a broad view of the environment.

The importance of a highly professional and capable analytical base for internationally oriented Polish business in the perspective we are presenting is therefore a central, key issue. It is not possible to be highly successful in foreign markets without incorporating knowledge of individual regions, states, and target markets into business operations. This knowledge must be as complete and up-to-date as possible but also accessible. An important component of modern strategic analysis must also be a sound analysis of threats and risks, which of course cannot be eliminated in business but must be understood and skilfully navigated.

Poland is a country that carries out a number of activities aimed at supporting Polish business internationally that are related to gathering and sharing knowledge about specific markets. The activities may also be initially considered to be scattered (several state institutions and organisations involved) and, at the same time, quite modest in terms of available budget and, consequently, actual impact. The urgent challenge is to coordinate the knowledge and actions of the various institutions and services of the state.

## 8. How should the unique strengths of Poles be used wisely in building international relations?

In the social sciences, the term "national character" is known to describe the relatively enduring characteristics and mental dispositions that recur within a given society and their regularity. In other words, researchers thus seek to understand what primary characteristics are typical of the representatives of a given national community. As far as the Poles are concerned, there are various studies in this area.

For example, there is very interesting research trying to summarise certain national patterns of Poles. We have a great tradition of the golden age of the Jagiellonians, when King Sigismund II Augustus stated that he was "*not a king of your consciences*." This statement captures very clearly what openness and tolerance are for Poles in the classic sense. There was no other country in the world like Poland during the difficult period of the Reformation and Counter-Reformation, there were no religious wars in our lands, no discrimination against any national minorities. Note that the Polish-Lithuanian Commonwealth was a state that lasted for more than four hundred years, which may support the hypothesis that such traits have been very strongly established in the Polish mentality[27].

Representatives of more than twenty nationalities lived in the borderlands of the Polish-Lithuanian Commonwealth. Poland was the country with the largest Jewish population in the

[27] P. Tarasiewicz, "Uniqueness of Polish as a nation" ["Specyfika Polaków jako narodu"], *Cywilizacja*, Vol. 37/2011, pp. 40-50.

world, who found a safe haven and great freedoms in our lands, mainly in the borderlands [Kresy]. One could say that Poland consciously embodied the idea of cultural pluralism, as that supported the pursuit of the idea of the common good in practice.

In fact, the Polish-Lithuanian Commonwealth was an avant-garde project in terms of integration ideas, significantly ahead of later ventures of a federalist nature, such as the United States of America or the European Union (sic!).

Perhaps, therefore, after the difficult period of communism, and then after a difficult period of a kind of indulgement in the mechanisms of the capitalist economy, the support for Ukraine and the very far-reaching solidarity shown in the face of the war tragedy seem to be another important turning point, an experience that is somehow formative, in the sense that it strengthens the strong points of the Polish mentality.

The considerable intellectual and social capital of Poles will support the development of Polish companies on the global market and will facilitate the building of a new opening in cooperation with any country in the world on the basis of long-term relations for which the pursuit of mutual benefits is important.

Genuine and honest practice of establishing business contacts (to use the language of management, the so-called networking) can become a driving force for the Polish economy. This is also the conclusion we are coming to with the Gospostrateg III project entitled: "Mazowsze akceleratorem globalnych przedsiębiorstw" ["Mazovia as an accelerator of global businesses"]. We note the indication by interviewees in the in-depth interviews conducted by the research team that it is crucial for business to build relationships based on trust[28].

## Conclusion

This article is an attempt to indicate, on the basis of preliminary research carried out within the framework of the Gospostrateg III project "Mazowsze akceleratorem globalnych przedsiębiorstw," that a new institutionalisation of modern strategic analysis may be of great importance at the state level.

Poland needs a more comprehensive, up-to-date, multidimensional, and business-accessible knowledge of foreign markets in all states of the world. Alongside a range of opportunities, these analyses must also include the identification of risks relating to international governance.

Poland is a rich country, we can afford a lot. The scale of the state budget provides the opportunity for huge projects to modernise the country. It is worth thinking about the future of the state using past experience in this area but also refining the approach. A key success factor may be the ability of Poles in international relations to build trust capital by developing partnerships based on mutual benefit.

---

[28] The Gospostrateg project has produced the first three project publications, each of which is relevant to the diagnosis of the situation and the recommendations formulated in this article. See: *Wyzwania związane z globalizowaniem mazowieckich przedsiębiorstw. Eksploracyjne badania diagnostyczne* [*Challenges of Globalising Mazovian Enterprises. Exploratory Diagnostic Research*], collective work edited by H. Rachoń and M. Wojtysiak-Kotlarski, OW SGH, Warsaw 2022; *Współpraca w ramach trójkąta relacji administracja-nauka biznes a wsparcie internacjonalizacji* [*Cooperation within the Triangle of Administration-Science-Business Relationship and Support of Internationalisation*], collective work edited by E. Pawęta, P. Pietrasieński, and M. Wojtysiak-Kotlarski, OW SGH, Warsaw 2022, as well as: *Uwarunkowania ekspansji zagranicznej przedsiębiorstw z województwa mazowieckiego. Analiza regionów światowej gospodarki* [*Determinants of Foreign Expansion of Companies from the Mazowieckie Voivodeship: Analysis of Regions of the World Economy*], collective work edited by M. Wojtysiak-Kotlarski, K. Kacperczyk, and A. Domańska, OW SGH, Warsaw 2022.

## References


Chang H-J., *Economics: The User's Guide*, Penguin Books, London 2014.

Chołaj H., *Powrót olbrzyma w zglobalizowanym świecie* [*Return of the Giant in a Globalised World*], OW SGH, Warsaw 2016.

Kołodko G.W., Świat w matni. Czwarta część trylogii [*The World in a Quagmire. The Fourth Part of the Trilogy*], Wydawnictwo Prószyński i S-ka, Warsaw 2022.

Leduff Ch., *Detroit: An American Autopsy* [*Detroit. Sekcja zwłok Ameryki*], 3rd edition, Wydawnictwo Czarne, Wołowiec 2019.

*Odkrywając wolność. Przeciw zniewoleniu umysłów* [*Discovering Freedom: Against the Enslavement of Minds*], Wydawnictwo Zysk i S-ka, Poznań 2012.

*Odkrywając wolność 2. W obronie rozumu* [*Discovering Freedom 2: In Defence of Reason*], Czerwone i Czarne, Warsaw 2022.

*Polish Deal*, https://www.gov.pl/web/polski-lad/o-programie

Rodrik D., *One Economics, Many Recipes: Globalization, Institutions, and Economic Growth* [*Jedna ekonomia, wiele recept. Globalizacja, instytucje i wzrost gospodarczy*], Wydawnictwo Krytyka Polityczna, Warsaw 2011.

*Strategy for Responsible Development by 2020 (with an outlook by 2030)*, https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju,

Szczaniecki M., Sójka-Zielińska K., *Powszechna teoria państwa i prawa* [*Universal Theory of State and Law*], Wydawnictwo Wolters Kluwer, Warsaw 2016.

Szymański W., *Interesy i sprzeczności globalizacji. Wprowadzenie do ekonomii ery globalizacji* [*Interests and Contradictions of Globalisation: Introduction to Economics of the Globalization Era*], Wydawnictwo DIFIN, Warsaw 2004.

Tarasiewicz P., "Uniqueness of Polish as a nation," ["Specyfika Polaków jako narodu"], *Cywilizacja* Vol. 37/2011.

*Uwarunkowania ekspansji zagranicznej przedsiębiorstw z województwa mazowieckiego. Analiza regionów światowej gospodarki* [*Determinants of Foreign Expansion of Companies from the Mazowieckie Voivodeship: Analysis of Regions of the World Economy*, collective work edited by M. Wojtysiak-Kotlarski, K. Kacperczyk, and A. Domańska, OW SGH, Warsaw 2022.

*Współpraca w ramach trójkąta relacji administracja-nauka biznes a wsparcie internacjonalizacji* [*Cooperation within the Triangle of Administration-Science-Business Relationship and Support of Internationalisation*], collective work edited by E. Pawęta, P. Pietrasieński, and M. Wojtysiak-Kotlarski, OW SGH, Warsaw 2022.

Ha-Joon Chang's lecture in the series Economics for People: https://www.youtube.com/watch?v=qaNTRFOkp0Q&list=PLmtuEaMvhDZbNVIDHA-MTVH0sLb5HP7Pn

www.un.org/ohrlls/sites/www.un.org.ohrlls/files/landlocked_developing_countries_factsheet.pdf

*Wyzwania związane z globalizowaniem mazowieckich przedsiębiorstw. Eksploracyjne badania diagnostyczne* [*Challenges of Globalising Mazovian Enterprises. Exploratory Diagnostic Research]*, collective work edited by H. Rachoń and M. Wojtysiak-Kotlarski, OW SGH, Warsaw 2022.

***Beata Wiśnicka***

*Independent expert. Graduate of the SGH Warsaw School of Economics. She completed an advanced AML course at The International Compliance Association in London. Board member at the Association of Certified Financial Crime Specialists – Central European Chapter. She serves as the MLRO for a Payment Institution. She has implemented AML and KYC processes for clients from: Poland, Lithuania, Latvia, the UK, Cyprus, Malta, Gibraltar, Panama, China, Australia. For several years, she has been involved in the world of cryptocurrencies. With her expertise, she has also supported banks in Switzerland. She designs customised AML solutions for companies in the process of obtaining a National Payment Institution licence. She has trained hundreds of AML experts in Poland. Originator of the YouTube channel "Jak nie dać się oszukać" ["How Not To Get Ripped Off"]. Mentor in the Perspektywy Women in Tech programme.*

# Correspondent banking

Correspondent banking remains an important alternative from an efficiency and cost point of view, which can be used when payments cannot be processed directly by the payment system or to make payments between systems. In fact, most payment systems cover the national market (i.e. the domestic market and the Eurozone market) and some integrated payment markets, such as the Single Euro Payments Area.

In addition, international banks with direct access to payment systems in different currency areas are rare, mainly due to restrictive rules on access to payment systems, as well as the cost of setting up branches and subsidiaries in other countries that can access the payment system. The correspondent banking network can be seen as a worldwide network of bilateral relationships, enabling a bank customer to make and receive payments in any currency from/to virtually any counterparty with a bank account. To this end, sometimes several correspondents may be involved in a single payment. It is certainly a rewarding solution for both banks and customers.

Customers of the respondent bank do not have direct access to the correspondent's account, but transact indirectly.

Correspondent banking can include various services such as:

- international transfers;
- clearing cheques;
- trade finance;
- loans;
- currency exchange services.

## AML processes in correspondence

In a correspondent banking relationship, the correspondent institution will monitor the transactions of the respondent institution in order to detect any changes in the respondent institution's risk profile or the implementation of risk mitigation measures (i.e. unusual activity or transactions on the part of the respondent or possible deviations from the agreed terms of the arrangements governing the correspondent relationship). In practice, where such concerns are identified, the correspondent institution will contact the responding institution with a request for information on any particular transaction, which may lead to a request for additional information on a particular client or clients.

The FATF Recommendations require financial institutions to identify, assess, and understand money laundering and terrorist financing risks and to implement AML/CFT measures that are commensurate with the identified risks.

Prudential and other regulatory requirements, as well as the complexity, number, and evolution of sanctioning regimes and the uncertainty surrounding the interaction of different sanctioning regimes and their application to financial institutions, have also been cited as reasons for risk mitigation. AML/CFT regulation is therefore only one of many factors identified as reasons for the closure of correspondent banking relationships.

When assessing the risk of their respondent, cooperating institutions must ensure that the assessment is sufficiently robust to address all relevant risk factors. In this way, the different levels of inherent risk are clearly understood and appropriate controls are applied to each, ensuring that these risks are managed effectively. Accordingly, the extent to which additional measures should be applied will vary from case to case, depending on the level or type of residual risk, including the measures that the respondent institution has implemented to mitigate its own money laundering and terrorist financing risks.

The factors to be considered when assessing correspondent banking risks may include, for example, the respondent institution's jurisdiction, the products/services it offers, and its customer base. For several reasons, it is not possible to develop a definitive list of types of higher-risk relationships. Firstly, there is no exhaustive list of risk factors that can be used to identify such relationships that would apply equally to all relationships. Secondly, both the relevant risk factors and the relevant mitigation measures must be considered together to create an accurate and comprehensive picture of the risk.

When establishing a business relationship, the correspondent institution should first identify and verify the identity of the respondent institution using reliable independent source documents, data or information. It should also identify and take reasonable measures to verify the identity of the beneficial owner(s) so that the correspondent institution is certain that it knows who the beneficial owner of the respondent institution is. For this purpose, the correspondent institution should also understand the ownership and control structure of the respondent institution. Information on the ownership and control structure includes carrying out a verification that allows the correspondent institution to become certain that the respondent institution is not a fictitious bank. In addition, the correspondent institution should gather sufficient information to understand the purpose and intended nature of the correspondent banking relationship.

This includes an understanding of the type of customers the respondent institution intends to serve through the correspondent banking relationship and how it will offer services, including the

expected level of business, volume, and value of transactions, the nature of the transactions planned, and the extent to which each transaction was assessed by the respondent institution as high risk. The correspondent institution should also gather sufficient information and determine from publicly available information the reputation of the respondent institution and the quality of its supervision, including whether (and when) it has been the subject of a money laundering or terrorist financing investigation or regulatory action.

In addition, the correspondent institution should assess the AML/CFT controls of the respondent institution. In practice, such an assessment should include a review of the respondent institution's AML/CFT systems and control framework. The assessment should include confirmation that the respondent institution's AML/CFT controls are subject to an independent audit (which may be external or internal). A more detailed/in-depth assessment should be carried out for higher risk relationships, possibly including a review of the independent audit, an interview with the compliance officer, a third party review, and potentially a site visit.

The correspondent institution should also understand how the respondent institution will offer its customers the services available through the correspondent banking relationship and assess the nature and level of risk associated with the offering arrangements. There are several possible solutions for offering services.

Correspondent banking relationships are **inherently based on mutual trust** between correspondent and respondent institutions, particularly as respondent institutions effectively implement AML/CFT controls. Accordingly, it is important that correspondent institutions maintain an ongoing and open dialogue with respondent institutions, including helping them to understand correspondents' AML/CFT policies and expectations and, where necessary, engaging with them to improve their AML/CFT controls and processes. Such communication supports the monitoring requirement, helping flagging new and emerging risks, and better understand existing risks, clarify in a timely manner any incidents that may occur during the course of the business relationship, reinforce risk mitigation measures, and resolve any issues that may arise from the exchange of information. This process can also help build the capacity of respondent institutions. It can also help avoiding unnecessary restrictions or terminations of relationships without a thorough assessment of the risks associated with a particular customer.

Correspondent banking relationships are very diverse in nature and therefore cover a wide range of high levels of risk. The level and nature of risk may change during the course of each relationship and adjustments should be made to the relevant institution's risk management strategy to reflect these changes.

***Anna Krop***

*Criminal analyst with several years of experience in law enforcement, analytical skills trainer.*
*The object of her interest is the use of modern technology to commit crimes and conceal identities.*

# "A Thing on the Internet? Or the Internet in a Thing? New Technology Crimes"

## Introduction

The article addresses the issue of crimes committed with the use of the Internet of Things (IoT), including possible threats in the area of new technologies in theoretical and practical terms. A close link is seen between the increasing use of modern online communication solutions and criminal trends, challenging both the direct prosecution of criminals and the identification and prevention of abuse. It seems to be largely underestimated in the process of fighting crime—both already at the stage of estimating the risks of its occurrence and in terms of a source of knowledge when uncovering criminal acts.

Despite the often-expressed opinion that the new technology crimes refer to some indefinite future, they are not somewhere out there but surround us in the here and now. This is because of the technological boom that we are witnessing and at the same time are beneficiaries of, which is

impossible to recognise, understand, and manage by a single person and often also by an entire organisation. It is fair to say that most plans to address IoT threats are outdated by design, as they stem from a reactive process of recognising and investigating dangers and the education cycle that those fighting crime have to go through. This problem is not faced by criminals, however, who adapt to change quickly, using everything they can. So any solution that can conveniently, quickly, and anonymously get them to their destination is highly desired by persons operating in the field of addressing IoT threats.

## Internet of Things

One way of defining the IoT is to describe it as a concept of combining the virtual and real worlds, based on three pillars that relate to the characteristics of smart objects. These objects (i.e. devices), must be able to recognise each other, communicate with each other, and cooperate with each other, i.e. influence each other's actions. In other words, the Internet of Things means no less than that not only people but machines and other devices will interactively communicate over the Internet.

Defining the Internet of Things as "simply the point in time when more things or objects were connected to the Internet than people," Cisco Systems estimated that the IoT was "born" between 2008 and 2009. In 2013-2014 it has been 3,8 billion devices, estimates of the scale of the Internet of Things in 2020 ranged from 20 billion to 110 billion devices, with 20-30 billion being the most common number. These are calculations by large IT companies, researchers, but also by state or EU institutions. The estimates for 2025-2030, on the other hand, are from around 2020. They conclude that the highest predictions did not come true but it is now possible to speak of well over 20 billion devices.

The range of equipment capable of operating within the Internet of Things is growing every day. It can be any device or a collection of devices that will be tasked with performing an action based on the data. These range from individual objects (sensors, light bulbs, cameras, sprinklers) to more or less complex systems (white and brown goods such as fridges, washing machines or televisions, research equipment, communications equipment), and finally, with advances in technology and increased data throughput, entire homes, neighbourhoods, institutions and cities.

The modes of connectivity of IoT devices will include traditional wired connectivity but the vast majority within the Internet of Things will involve well-known radio transmission modes, within: local area network, Wi-Fi, bluetooth, cellular network (5G), which do not require a specific description of how they work.

IoT devices also commonly communicate using a communication standard such as Zigbee or similar technologies. It is a data transmission protocol for wireless networks that can be compared to Wi-Fi but is characterised by: lower power consumption, low bit rates (up to 250 kbps), and a range between nodes of 100 m. Typical applications are sensor networks, personal networks (WPAN), home automation, alarm systems, monitoring systems. Communication in ZigBee is two-way, meaning that any device can receive or send a signal and some can even pass it on. Its advantages also include instant access, which is why it is readily used in such devices as motion sensors. ZigBee was developed with the idea of low data transfer rates and thus relieving the burden on Wi-Fi. When it is enabled, devices typically report information such as battery level or connection quality, sending a signal that something is happening. However, it is not suitable for audio or video transmission due to the volume of this type of data.

## Benefits, vulnerabilities, risks

We should first highlight the benefits of creating high-speed communications (such as 5G) or those that do not require high bandwidth (such as ZigBee). It is certainly a technological development that aims to improve the quality of human life by e.g.: increasing convenience and comfort, saving time or energy, making work and life easier, supporting elderly people to live independently, caring for the environment, optimising production processes or improving safety.

However, almost every change or discovery brings with it not only advantages but also disadvantages. IoT devices communicating over low data technologies are characterised by their small size, narrow purpose, small memory, the need for unencumbered data transmission, and the desire to save energy. In contrast, devices connecting via 5G are commonly placed in locations that are accessible to the general public, often without the application of service availability restrictions. In the face of all these facts, the Internet of Things facilities are vulnerable to hacking, data interception, and remote or physical takeover.

The first years of IoT development can be compared to the development of the Internet itself—first and foremost, it was supposed to work. At the stage of its hatching, safety was not the concern it is now. Therefore, communication standards such as ZigBee, that are specially created for devices, very often do not even provide a minimum of security for data transmission. They are not secured properly or at all, e.g. they have open ports, the factory settings and passwords are not changed or they have no passwords at all, the transmission is not encrypted in any way. The 5G SIM cards used in the devices, on the other hand, are sometimes unsecured at the card-enabled level and have no restrictions on the use of services or limits on calls or messages sent.

The potential for hacking and further exploitation is therefore enormous and, due to the number and specificity of the devices, even much greater than for computers alone. It is easy to imagine that once the owner of a device or network has gained illegal control of it, other individuals and businesses, public institutions, and any organisation are exposed to many risks. And according to estimates from a few years ago, more than 70% of IoT devices contain hacking vulnerabilities.

Threats emanating from such hacking include: access to home appliances and monitoring, interception and use of personal data, extortion or theft of funds from payment cards or SIM cards directly connected to devices, blackmail and harassment regarding business downtime (e.g. fridges raising temperatures, transport blocking, parcel delivery equipment paralysis) or data security (e.g. attacks on banks), or theft of company secrets. Another threat could be crimes against health and life or terrorist threats (e.g. in the energy sector or public transport). It is also important to note the change in the scale and characteristics of the crime, with such devices "entering the game." This means the emergence of new opportunities and therefore a modification of the criminal's modus operandi. After all, it will be different to be exposed to a loss of privacy if we lose data from a computer or someone peeps at us with their camera, as compared to a situation when someone gains data about our preferences and habits based on the TV channels we watch and locations stored on our devices, has access to surveillance cameras, an electronic nanny or even a cleaning device or yet other household appliances.

## Experiments

There have been a number of scientific experiments regarding IoT threats involving breaking through security and gaining access to devices.

One is the spectacular example of a Jepp Cherokee that was planned to be remotely hacked and taken over. After analysing its equipment, the attackers found one unsealed port in the on-board entertainment system, which allowed for a remote connection and subsequent access to the CAN bus, through which all the car's equipment could be controlled. The attackers took control of, among other things, the steering wheel and brakes, as well as the utility systems (air conditioning, windscreen wipers). Although the driver was aware of the experiment, they were shocked by the loss of control. As a consequence of the experiment, the car's manufacturer asked its owners to contact them to fix the security gap. Although no accident occurred and the attack could not be repeated after adjustments to the settings, the fact that it was possible in the first place worried all car manufacturers. Until now, Internet connectivity had been advertised as an asset, meanwhile, people begun to be concerned about the dangers of remotely taking control of the vehicle. This could include smashing it into an obstacle, diverting it into a collision course with another car, hitting a pedestrian or trapping the driver and passengers in the car.

Another example are two experiments on the safety of hospital drug dispensers. These devices are usually connected to hospital networks, hooked up to the internet, and are used to administer drugs to patients, the dosages of which are specified in file libraries stored on the device. Both attacks succeeded by breaking security, after which: during the first one, the drug dosage was increased within the limits specified in the factory file library, while any changes above this dosage resulted in an alarm; and in the second one, the attackers managed to swap the files in the library with those containing the increased permissible drug standards. That allowed the drug dose to be set at a level that posed a risk to the patient's life. In addition, the information displayed on dispenser screen indicated that the dose was within normal limits. The identified vulnerability was the acceptance of any software update, added by any unauthorised person, rather than those with appropriate access (such as an employee of the software manufacturer or hospital). In the case of patients in a serious condition, perhaps a murder would not even be suspected.

Risks concerning medical equipment also apply to e.g. personal insulin pumps. A while ago, one of their manufacturers announced that the pumps they produced could be hacked. The communication between the pump and the remote control was not encrypted, and someone familiar with the device, standing a few metres away from a diabetic, could tap into it and then administer additional doses of insulin to the patient. That could be used for blackmail, death threats or even really to deprive someone of their life.

## The Internet of Things in the media

Plots involving remote hacking of domestic and medical devices or vehicles have been present in mass culture for many years, mainly in films and TV series. One such example is the script for the second season of the TV series *Homeland*, in which one episode features terrorists killing the Vice President of the US using his pacemaker. The device connects via radio waves to the software that controls its operation. The terrorists take it over and trigger the politician's fatal heart attack. Is this just the fantasy of Hollywood scriptwriters? Well, not necessarily: in 2007, after having a pacemaker inserted, the then US Vice President Dick Cheney decided to determine whether a cyberattack

threat was possible. Because he had heard from the specialists that it was, he ordered that the possibility of wireless communication with the pacemaker be turned off. The purpose of equipping these types of devices with connectivity is to allow the doctor to remotely monitor the patient's condition and also to save lives in an emergency by sending a pulse to restore normal heart function. However, due to the small size of pacemakers, they do not have security features to encrypt the connection. Dick Cheney only admitted to abandoning the remote connection in 2013, after the aforementioned episode of the series had already aired. In contrast, the possibility of hacking pacemakers has been proven by experiments on phantoms showing that the heart rate can be influenced and, if the pacemaker is equipped with a remotely activated defibrillator, it is possible to send a command, triggering controlled electrical shocks to manipulate the artificial heart.

## Summary

For years, the hacking community has been discussing the use of IoT for its own purposes—that is, reaping the financial benefits of attacking internet-connected devices. To make money, hackers sell access to devices, like routers, webcams, and printers, that can be used for attacks. Therefore, they can sell access to any device or prepare it for a proper attack.

In contrast, by driving vast amounts of information into cyberspace and transferring responsibility for activities and processes to machines, people are living more comfortably while exposing themselves to new risks. It takes time and practice to create effective safeguards. As in almost every case, building security is about the pursuit of the criminal world and its methods of operation, and the Internet and related technologies supply criminals with new opportunities to act, exposing the vulnerabilities and susceptibilities of the information society.

***dr hab. Kacper Gradoń***

*University lecturer, expert in forensic science and criminal analysis,*
*adjunct professor at the Warsaw University of Technology,*
*research fellow at University College London*
*and the University of Colorado Boulder.*
*Division of Cybersecurity, Warsaw University of Technology.*
*kacper.gradon@pw.edu.pl*
*Department of Security and Crime Science, University College London.*
*k.gradon@ucl.ac.uk*
*University of Colorado Boulder, Prevention Science Program.*
*kacper.gradon@colorado.edu*

# Disinformation and Artificial Intelligence Techniques—a Double-Edged Sword?

The infodemic is one of the most pressing problems in the world today, which is recognised by international organisations—both civilian ones, such as the United Nations agencies (World Health Organisation and UNESCO) or the European Union institutions (European Parliament, European Commission), military organisations (NATO), and police or intelligence organisations (EUROPOL, Interpol). An infodemic is a concept that describes the overload of informa-

tion—both true and false—that determines the perception of the world by its recipients, which is particularly relevant during crises of great (national, regional, global) importance and scope. This term includes several subcategories—understanding and distinguishing between them is important for developing appropriate prevention and mitigation strategies. Disinformation is false information that is deliberately created and disseminated with the express intention of causing harm; fabricated content and malicious intent behind it are the distinguishing features of disinformation. The term "misinformation" is often erroneously used as a synonym for disinformation but although the information disseminated in this case is also false, it is not intended by its authors to cause harm because those sharing it believe it to be true and accurate. Finally, the so-called malinformation is truthful information that is disseminated with the express intention of causing harm (e.g. by revealing sensitive, private data that may damage the reputation of a particular person, company or institution).

Disinformation and misinformation are not new phenomena but recent events such as the COVID-19 pandemic, the unprovoked military aggression of the Russian Federation against Ukraine or the growing tensions over the territorial claims of the People's Republic of China against the independent Republic of Taiwan have undoubtedly contributed to a marked increase in the propagation of harmful, false or misleading information at a global level. It should be emphasised that all kinds of crisis situations, including natural disasters, periods of social unrest and tension, political events of supranational importance or significant macroeconomic changes, provide a breeding ground for disinformation and can become a tool for information operations as part of broader military strategies. This kind of action is nothing new but we are now faced with a much larger scale of such problems and incomparably more powerful possibilities for their rapid dissemination.

We have seen a steady increase in the reach and importance of electronic media over the years but we are now experiencing unprecedented (over many decades) global epidemiological, economic, and military threats with all their social, economic, and political consequences. They become an ideal breeding ground for the creation and dissemination of various conspiracy theories, intensify the propaganda activity of a wide spectrum of extremist movements, and provide ideal opportunities for organised (state-controlled and controlled) campaigns categorised as elements of information warfare (which is, as it should be particularly pointed out, the speciality at the state level of the Russian Federation and the People's Republic of China). Electronic media and, above all, social networks favour the extremely rapid propagation of all kinds of information, and lead to the perpetuation of so-called information bubbles, i.e. situations in which a group of people have limited knowledge of a phenomenon and their beliefs and views about it are mutually reinforced by the media or social narrative accompanying them at a given time. Consequently, such people only accept as true information and opinions that confirm their previous beliefs and reject those that do not fit their vision of the world. Information bubbles lead to misunderstandings, prejudices, and conflicts between different groups of people who have different views on an issue. Social network users operating inside such environments tend to ignore facts that challenge their beliefs, making it difficult to reach consensus and solve social problems. Modern social media, by allowing users to access personalised content and suggesting similar content to what they are already viewing, contributes to the importance of information bubbles, which consequently become an excellent tool for creating, amplifying, and further disseminating disinformation content.

Disinformation campaigns primarily serve states with an interest in undermining democratic systems of government and sowing unrest and chaos in the societies targeted by such attacks. This helps the authorities of the states inspiring and sponsoring disinformation to achieve their strategic, geopolitical goals. In the case of the Russian Federation, this is primarily about the practical implementation of a strategy of hybrid warfare (the so-called Gerasimov doctrine) and the destabilisation of Western societies; for China, the motivation is the desire to acquire the key role of world superpower and economic dominance. At a slightly lower level, disinformation campaigns also serve extremist groups (both on the left and right of the political spectrum) which use these methods to deepen polarisation and divisions in society. Indeed, it is a favourable intermediary tool for state-controlled disinformation strategies (the activities of competing extremist movements within a country can be fuelled by a hostile state, as we witnessed in 2020 in the United States where the Russian Federation simultaneously inspired opposing sides of the conflict in the run-up to the presidential election; according to counterintelligence institutions, similar strategies were already used in 2016 during the US election campaign, and during the British referendum related to the prospect of the UK leaving the structures of the European Union, as well as in 2018 during the so-called "yellow vest" protests in France).

From the perspective of international institutions, the most serious threat is precisely the strategy of hybrid warfare where public sentiment is controlled and public opinion is manipulated with methods of disinformation, undermining the legitimacy of international organisations and alliances (European Union, NATO, WHO). The dissemination of fake news also has a direct negative impact on national and international strategies, a recent example of which (during the COVID-19 pandemic) was the undermining of universal public health procedures, which were destabilised by the activities of anti-vaccine movements stimulated using disinformation techniques. Currently, in real time, we are seeing these kinds of threats in relation to the ongoing consequences of the war in Ukraine, where the Russian Federation is using disinformation strategies as an important element to complement the "kinetic" side of the conflict. Criminals (including organised crime groups) as well as terrorist organisations are also exploiting the fear, anxiety, and uncertainty associated with crisis situations by intensifying activities that fall into the broad category of cyberattacks (including cyber-enabled attacks, where information technology is used to prepare and execute real-world operations), creatively repurposing existing methods into ones that take advantage of the circumstances and social impact of specific types of threats. And in such cases, we are dealing with the use of manipulative techniques using methods that can be categorised as disinformation activities. Fake news disseminated via electronic media (including, in particular, social media) also poses a very serious threat to economic security (at the macroeconomic level—e.g. when confidence in the stability of strategic sectors of a particular country's economy is undermined), as well as to the safety and conduct of business activities carried out by entrepreneurs (unfair competition using disinformation methods to undermine the quality of products or services offered by the targeted company). Disinformation can also directly affect specific individuals, when defamation campaigns amplified with social media can translate directly into loss of reputation and tangible personal, financial or professional damage.

One of the biggest challenges facing national and international institutions tasked with countering disinformation is how to tackle the vast amounts of data that need to be analysed. The flow of information, which includes a wide range of narratives, both true and false, cannot be analysed quick-

ly, accurately, and efficiently by trained professionals alone, even with the support of fact-checking organisations. While the work of fact-checking institutions and organisations should be supported and appreciated, it should be noted that the amount of data needed to be analysed in real time and retroactively makes such a traditional analytical approach virtually impossible (at a holistic and strategic level) and sometimes even counter-productive. The ability to analyse large datasets from different types of media (traditional, electronic, and social media), collected at international, national, regional, and local levels and supplemented with spatial-temporal data, related to demographics and mobility, must rely on the use of appropriately calibrated information technologies. However, by the very nature of such technologies, they have the characteristics of a "double-edged sword"—i.e. their effectiveness in detecting disinformation means that, once properly calibrated, the same tools can be used to create and propagate harmful and dangerous content.

Currently, the most practically relevant automated technologies applicable to both the creation and detection of disinformation content are based on Artificial Intelligence (AI) and Machine Learning (ML) algorithms. Of these, the techniques of the so-called (GANs) and Large Language Models (LLMs) are of particular relevance in the field.

Generative Adversarial Networks are machine learning models consisting of two competing neural networks, called a generator and a discriminator. GANs are used to generate new data samples, such as images, sounds or text. The generator creates data samples and the discriminator classifies whether they are real or artificially produced. The two neural networks learn from each other and strive to reach an equilibrium where the generator will produce reliable samples of data that the discriminator cannot distinguish from the real thing. GANs are used in many fields such as image processing, animation, synthetic data generation, and natural language processing. In the case of disinformation, possible uses of GANs include the creation of fake textual content (as well as graphics, videos, and audio). In such a case, the generator may learn to create false content that looks and sounds like the real thing and the discriminator may not be able to detect it. On the other hand, GANs can also help to detect disinformation. Neural networks can learn to recognise false content that has been generated using other GANs, making it possible, in theory, to identify and then remove, flag or unmask false information.

Large Language Models (LLMs) are a type of machine learning algorithms that have the ability to generate natural-sounding texts. LLMs are learned from huge linguistic (textual) corpora and can generate texts in a way that seems natural to the audience. As a result, they are able to understand the context and meaning of words and relate to existing knowledge and experiences. LLMs are used in many areas, such as machine translation, generating photo descriptions, writing articles and reviews, and creating chatbots. Thanks to their ability to generate natural-sounding text, they can be used in a variety of situations where generating text at the "human-level" is required. However, they can also pose a risk, particularly in the context of disinformation, as, due to their ability to generate natural-sounding text, they can be used to create very plausible-sounding and linguistically correctly written false information that can effectively mislead audiences. In theory, LLMs can also provide a tool for disinformation detection, e.g. by harnessing these technologies to recognise, analyse, and classify texts, as well as to create solutions for subsequent fact-checking. The use of LLMs in the fight against misinformation is problematic, however, as these models may start to repeat and propagate existing errors or false information that existed in the training data available to them.

Currently, the best and most up-to-date example of a solution gaining popularity based on Artificial Intelligence and Machine Learning technologies is ChatGPT. It uses Large Language Models (LLM) concepts that have been carefully trained on huge datasets, and Generative Pre-trained Transformer 3 (GPT-3) technology. GPT-3 is OpenAI's machine learning-based neural network with a capacity of 175 billion parameters, ten times that of the nearest comparable system, Microsoft's Turing NLG. The power of the OpenAI model comes from the advanced initial training and the scale of this process is well illustrated by the fact that Wikipedia's resources represent only 3% of the hundreds of billions of words used to train the model. ChatGPT uses Supervised Learning and Reinforcement Learning technology. It is designed as an advanced chatbot that can support a wide variety of language applications and its main advantage is its tremendous speed and ability to understand complex and nuanced commands from the user in multiple natural languages. ChatGPT stands out for its great sophistication and speed in creating textual content that is persuasive, logical and follows the rules of language, style, grammar, and spelling. As such, it has great potential for multiple levels of criminal abuse of technology. It gives, for example, the ability to create very realistic and convincing phishing messages that are difficult to distinguish from real and harmless messages. It can also be used to create false disinformation content quickly and effectively.

The availability of such advanced technology, which can easily be used for criminal and military purposes, poses a huge challenge to law enforcement and intelligence and counter-intelligence services. The unprecedented quality of such tools combined with their low cost, wide availability, and ease of use will lower the "entry threshold" into the criminal market. An additional problem is that crimes related to artificial intelligence and machine learning technologies (such as ChatGPT just now) are highly scalable and such techniques can be shared, repeated or sold. The growing potential for the commercialisation of criminal techniques using Artificial Intelligence and Machine Learning should also be highlighted. AI/ML abuse fits here into the category of "Crime as a Service" threats, where competent cyber criminals can design, offer, and sell IT tools to other criminals with limited technical skills. Additionally, organised crime groups, extremist and terrorist organisations or hostile states, rather than employing people to design, write, and propagate disinformation content, can themselves use ChatGPT-like technologies to create realistic, convincing, and varied false and damaging information on a huge scale and with great effectiveness.

In order to effectively counter such threats, efforts should be made to build a set of IT tools (using artificial intelligence, data science, and machine learning techniques, as well as intelligence analysis and natural language semantic analysis) for proactive detection and flagging of false information in electronic media, as well as tracking of its propagation paths, identification of nodal points, and the ability to determine the original sources of disinformation. Such tools (exemplified by the research and implementation assumptions of the Polish Infodemicon project) should support government agencies, health care providers, the news media, NGOs, and the private sector, allowing automated processing and analysis of information for early detection of potential threats. The use of AI tools has the potential to identify sources of disinformation, study how disinformation travels through networks, and ultimately mitigate the effects of disinformation. It is possible to test these methodologies in the context of disinformation regarding COVID-19, vaccination against the SARS-Cov2 virus, and broadly based on disinformation linked to the war in Ukraine. Many of the disinformation sources in these cases are well known, making it possible to validate AI techniques

and train AI tools. The effect of implementing such solutions should be to contribute to reducing the negative impact of disinformation and limiting its propagation, which should translate directly into reducing the possibility of manipulation of public opinion by criminal groups, terrorist and extremist organisations, and, above all, the intelligence services of foreign countries hostile to our values and international alliances.

## References:


Kacper Gradoń and Wesley R. Moy: "Artificial Intelligence in Hybrid Warfare – a Double-Edged Sword" in: *Artificial Intelligence and International Conflict in Cyberspace* (Eds. F. Cristiano, D. Broeders, F. Delerue, F. Douzet, and A. Gery). Routledge, Milton Park (UK). In print (May 2023).

Kacper Gradoń: "COVID-19 and the Information Ecosystem. Lessons from the Russian Malign Influence in the Post-Covid-19 World" in: *A World Emerging from Pandemic: Implications for Intelligence and National Security* (Eds.: S.E. Pollard and L.A. Kuznar), National Intelligence Press (USA), 2022.

Kacper Gradoń: "Electric Sheep on the Pastures of Disinformation and Targeted Phishing Campaigns. The security Implications of ChatGPT." In: *IEEE Security & Privacy*, Vol. 21 Iss. 3, May-June 2023. DOI: www.doi.org/10.1109/MSEC.2023.3255039 In print.

Neville Calleja et al. (incl. Kacper Gradoń): "A Public Health Research Agenda for Managing Infodemics: Methods and Results of the First WHO Infodemiology Conference." In: *JMIR Infodemiology Journal* Vol. 1 No 1, 2021. DOI: doi:10.2196/30979

Kacper Gradoń and Wesley R. Moy: "COVID-19 Response – Lessons from Secret Intelligence Failures." In: *The International Journal of Intelligence, Security, and Public Affairs* Vol. 23, Issue 3, 2021. DOI: 10.1080/23800992.2021.1956776

Kacper Gradoń, Janusz A. Hołyst, Wesley R. Moy, Julian Sienkiewicz, and Krzysztof Suchecki: "Countering Misinformation: A Multidisciplinary Approach." In: *Big Data & Society, Special Issue on Studying Infodemic at Scale*. Vol. 8, Issue 1, May 2021. https://doi.org/10.1177/20539517211013848

Wesley R. Moy and Kacper Gradoń: "COVID-19 Effects and Russian Disinformation" in: *Homeland Security Affairs* 16, Article 8 (December, 2020) www.hsaj.org/articles16533

Kacper Gradoń: "Crime in the Time of the Plague: Fake News Pandemic and the Challenges to Law Enforcement and Intelligence Community" in: *Society Register*, 4(2), 133-148. https://doi.org/10.14746/sr.2020.4.2.10

***dr hab. in legal sciences Wojciech Filipkowski,***
***Professor of University of Bialystok***

*Head of the Forensic Laboratory of the Department of Criminal Law and Criminology at the Faculty of Law, University of Bialystok.*
*Scientific Secretary for Cooperation with Western Countries of the International Centre for Criminological Research and Expertise.*
*Author of more than 160 scientific publications on criminal law, criminology, and forensic science published nationally and internationally.*

# Proposed Assumptions for the Education of Strategic Analysts: A Contribution to the Discussion

Strategic crime analysis consists of: identification of the ways in which different categories of crime are carried out and their trends, threat assessment, assessment of the likelihood of their occurrence (risk assessment), and identification of factors external to the organisation, such as demographic, economic, social, and technological changes and their impact on crime or on the functioning of law enforcement or intelligence services. The definition of this concept brings us closer to the elements of the analyst's training process. The process should address the methods and techniques for carrying out the analysis and the factors affecting change in the long term. In addition to its descriptive and predictive purpose, its prescriptive (postulatory) nature is emphasised here. The proper application of the methods and techniques of conducting the analysis leads to the selection—according to the criterion of efficiency—of legal and organisational solutions that are likely to best prepare for the challenges of a changing reality.

Strategic crime analysis focuses primarily on one category of challenge, namely crime (or selected categories of crime). These are conceptual categories and objects of study primarily in criminology but also in forensic science and law. This definition lists the ways in which crimes are carried out (forensic techniques and tactics) and the trends in this area but also other challenges, which are sometimes threats that can potentially have a negative impact on the functioning of the organisation within which the analyses are prepared. Analytical techniques, i.e. threat assessment and risk assessment, are also explicitly mentioned.

Let us ask ourselves: what does the effectiveness of the analyses depend on? Like most professional human activities, this depends on a triad of factors: a suitably educated and prepared person, developed methodologies for proceeding, and suitably sophisticated tools used by a person when carrying out the methodology.

Let me distinguish 2 groups of characteristics or circumstances related to the analyst. These are those circumstances over which we have no control but are still desirable and can influence the choice of analyst candidates and those over which we have direct or indirect influence. The first group includes personality traits such as talent, good memory, curiosity, confidence, creativity,

openness, diligence, patience and perseverance, and passion. They result from conditions, e.g. biopsychology or upbringing. The second group consists of 4 subgroups. Firstly, there are the skills that can be more or less developed or honed: the ability to work independently, to collaborate in a group, which is what strategic analysts should do, to think analytically, to create analytical products efficiently, and to use software. Secondly and thirdly, they are, respectively, profiled (in a variety of scientific disciplines) and specialised education. Fourthly, it is professional experience (e.g. related to the implementation of analytical, operational or investigative activities).

As far as the educational process is concerned, as an academician-teacher, I declare my readiness to provide support in this area (but I believe I am also speaking on behalf of my fellow academics). Admittedly, we are not in a position to provide work experience to analysts but as academics, we can provide help in its research and scientifically development for further training to improve its effectiveness.

One of perhaps the key skills on the analyst's side is the so-called "soft" skills. One might even be tempted to say that some people are born with them, while others have to develop them for themselves. The process of training an analyst should, of course, include a selection element, where those with already developed competences should find their application in performing analytical work. On the other hand, it should also be up to law enforcement agencies and services to continuously improve these skills through various types of specialised and professional training.

Firstly, it seems obvious that for analysts, a rational approach to investigating and solving the problems that will be set before them is crucial. This of course requires thinking, not only logical (classical) thinking, but also out-of-the-box thinking, i.e. thinking creatively, being critical of the results of one's work by controlling the process of arriving at solutions and the results themselves, and constructive thinking, i.e. actively seeking even better solutions to these problems. Secondly, we live in an information society and one of the basic modern skills is the search for and evaluation of data and information. The last and, in my opinion, very important skill is the so-called time management.

Another triad I would like to present concerns teamwork. Taking into account the literature and the results of the research, it can be concluded that in the case of strategic analysis, it should be carried out in teams. Now the question arises: what should be the optimised composition of such a team? This triad includes three categories of people according to their knowledge, skills or speciality. Firstly, it should include someone who has area knowledge of the issue. It includes knowledge from selected academic disciplines and professional experience. Secondly, we need a person who is knowledgeable about the data operating inside the institution and from external sources. Thirdly, you need someone who has knowledge of the broad tools that can be used to conduct research or analysis. I will only add that these people can be internal experts as well as external experts. They may come from outside the organisation and will then act as consultants, as far as legal considerations and organisational factors (e.g. related to access to state secrets) allow.

The second group of problems relates to areas, perspectives or scientific disciplines whose achievements can be used in the framework of ongoing research and strategic analysis. I will remind the concept of the scheme of the analysis process of Professor T. Aleksandrowicz consisting in the search for the answer to the questions: "What?" "And what results from it?" If we ask ourselves "What?," we are first of all asking about the past and the present: What was? And what is now? In the context of the issue we are investigating; What remains hidden for our knowledge about this issue?

What should we still discover? And why was it so and why is it so now? What in the past has led to the present state? In the context of crime, this is the primary focus of criminology in the areas of phenomenology and aetiology. The next step is to try to answer the question about the future: what will happen? The study of historical cause-and-effect relationships is therefore of great importance. The second step is to answer the question: what is the result of the knowledge thus gained and verified for the operation of the entity within which the research is conducted? Specifically, this concerns the issue: how do we prepare it for the changes that are likely to come? What resources that it has at its disposal (or does not have yet but should) will be most effective? The analytical product will propose courses of action and support the decision-making process.

People come to serve in law enforcement and intelligence services with a background in various higher education institutions (fields of study). Optimally, in the context of our considerations, it would be preferable to take on people who have a relevant body of knowledge, related to research methods and analytical techniques or technological solutions, about crime (or more broadly, threats against the state or society). Why optimally? Because in such a situation, the services does not have to "waste time" on further training on basic issues but can move on to "shape" the officer to their needs. Besides, the more diverse in terms of fields of study the analytical team is, the better, as each member will bring a different perspective on the problem under study of one crime or another, different research methods, etc. The important thing is that "in total" they will complement each other giving a synergistic effect.

The second stage is specialised education. It may be basic, universal for any function that an officer may perform in the future in a particular entity. However, they can already be both selected and educated in selected areas, which is actually done in practice (e.g. crime analyst courses). On the other hand, specialised education at an advanced level should already concern selected officers and highly specialised areas: analytical techniques, software.

I see four main areas for higher education institutions to get involved in the training of strategic analysts. For obvious reasons, higher education institutions have the capacity in the form of staff resources to carry out all kinds of learning processes. We can prepare candidates for service within the fields of study and specialisations provided for in the curriculum. We can also lead or co-lead specialised training courses on selected research methods and analytical tools or share our area knowledge. An interesting form is commissioned postgraduate courses, i.e. "tailor-made" for specific audiences. This offers the opportunity to meet the educational needs of law enforcement and intelligence services comprehensively and concretely—anywhere, i.e. at the higher education institution or the schools and training centres of these facilities, but also in the form of e-learning (in the form of so-called blended learning).

In contrast, a somewhat undervalued area is the use of the expertise of the higher education institution's research and teaching staff. We are outsiders to an institution, so we are often unfamiliar with its peculiarities, its limitations and its possibilities, but our innate or learned curiosity, the objectivity of doing research prompts us to ask questions, organise knowledge, look for gaps and fill them. Familiarity with phenomena, foreign solutions or scientific discourse allows the introduction of "creative ferment" into many discussions. I see opportunities to co-create training courses and thematic seminars and to develop training materials for the educational process. We can also give our opinion on existing training programmes and suggest changes that correspond to the current state of knowledge on a given problem within our scientific competence.

Another area is conducting research for the client. The research may concern the problem or phenomenon itself but also the study of the educational process, the development of research and analytical methods, the scientific development of good practices, etc. I would like to also emphasise the importance of criminological, forensic, and legal research in the context of the preparation and implementation of technological solutions into the practice of law enforcement and special services to fight crime.

To summarise, the most important considerations of the strategic analyst education process, in my opinion, include:

- stakeholder cooperation in basic and specialised education;
- diversity in such areas as: training providers, profiled education, composition of analysis teams, sources of data and information;
- the analytical product should support the decision-maker in the decision-making process with often out-of-the-box proposals but it should also be truthful and not just meet the decision-maker's expectations;
- the "soft" skills are at least as important as the "hard" ones.

***Jarosław Wolski***

*Polish political scientist, journalist, writer, and OSINT civilian analyst*
*Since 2014, he has been involved in the defence journalism industry in Poland, first with the website Dziennik Zbrojny, then the periodical "Dziennik Zbrojny. Analiza", and since 2015, with "Przegląd Sił Zbrojnych" and as a regular contributor (to date) with "Nowa Technika Wojskowa", (2016) "Wozy Bojowe Świata", "FragOut!" (2018).*
*Journalist for Magnum-X ("Nowa Technika Wojskowa") and "FragOut!"*
*Associated with the OSINT industry.*
*Married since 2011 with a son, a keen photographer, and a lover of bushcraft and industrial tourism.*

# "Open-Source Intelligence" (OSINT): the Development, Types, Capabilities, and Limitations of the Method of Obtaining and Analysing Information Extracted from Open Sources.

First we should answer the question: What is OSINT? In simplest terms, it is open-source intelligence based on completely open and publicly available sources. In other words, OSINT is as old as

humanity and its movement for the purpose of trade or travel. Besides, this dual role of traders and travellers was common and well known and their accounts of neighbouring countries (but not only) have always been a valuable and complementary source of information. The Industrial Revolution, the domination of the world by Europeans, and the subsequent development of press agencies, correspondents, etc. made "open-source intelligence" commonplace. The Great War and the era of totalitarianism that followed made such a method of obtaining information—especially against the USSR—less useful than in democratic countries. Totalitarian regimes were an extremely hostile environment for obtaining valuable information from open sources. This was due to the absence of such sources or the systemic falsification of officially available data. From steel production to crop acreage and fertility of married couples to immunisation, totalitarianisms massively altered data: either to build a more favourable picture of the system or to hide hypothetically sensitive data as part of systemic paranoia. Nonetheless, the OSINT methods—albeit with a very large margin of error—were also used in the bipolar times. Open-source intelligence returned in a big way with the demise of the rivalry between the Western Bloc and the Eastern Bloc and the formation of a multipolar world order, compounded by globalisation on the one hand and digital evolution on the other. The growth of the Internet and social media has brought OSINT into its golden age in terms of ease of access to data—both quantitative and qualitative. As a result, there has been a kind of "indulgence" in open-source intelligence. The Russian aggression against Ukraine caused OSINT to enter the mass media and become a popular term recognised even by those uninterested in the subject, while within the framework of rapid commercialisation, various "courses" teaching the collection and processing of information from open sources began to pop up like mushrooms. Is "open-source intelligence" in its contemporary form really such a useful tool?

To answer the above question, we have to ask ourselves about the sources of data and how access to them has developed two main types of OSINT. The sources of data are extremely broad, examples include: social media, newspapers, television, specialist periodicals, logistics systems, IP webcams, commercial satellite imagery, open and official government data, online forums, young pensioner's memories, commercial databases, etc. The apparent multiplicity of sources makes their selection and verification crucial. And here it is necessary to move on to explain the difference between qualitative and quantitative OSINT.

The former is based on the search for and verification of valuable information on particular problems, e.g. a given type of military equipment, the structures of the armed forces, arms production, conclusions from the battlefield, etc. In other words, in this case we are talking about the analysis of a certain narrow issue on the basis of a relatively small amount of data. As a result, the quality of reports usually depends on the experience and knowledge of the analyst who developed the issue.

Quantitative OSINT relies on the brute computing power of computers and access to possibly large numbers of databases grouping together personal data, social media images, etc. Here, the funds allocated have a relatively simple translation into the quality of the reports. The richer an organisation's portfolio, the better the software running on BigData and the more databases available. Of course, quantitative OSINT is by far more common at the level of government institutions, as it has been heavily developed in the age of the terrorist threat based on, for example, data from city surveillance cameras or databases. As a result, it is generally used universally but by the "strong" players i.e. the services or the wealthy multinationals. As such, however, it will not be the subject of this article.

Going back to technical OSINT—it has many advantages from the point of view of supporting the state security system. Firstly, it is low-cost insofar as the contracting institution tries to reach analysts bypassing consultancies that usually apply very high mark-ups. On the Polish market, a typical rate for a technical analysis by an analyst or a team of 2-4 analysts does not exceed PLN 30K net. Their analysis, after some light stylistic and graphic editing, then arrives on the table as a proposal from a b2g[29] consultancy with sometimes a zero at the end as the initial proposed price for the study. Secondly, OSINT is very much an "outside the box" view of the organisation. An external perspective can often provide many interesting insights which are then verified by the contracting institution. The aim, of course, is not to compete with or undermine the work of government institutions but to double-check an issue using a different research method. This translates into more certainty in the studies and therefore safer diagnoses. The modern "open-source intelligence" is also very effective especially in describing issues from democratic countries with civil societies, and it is also highly effective in describing specific issues in authoritarian countries, where the discipline of policing information is temporarily low and the spread of social media is very high.

When using qualitative OSINT, we should also bear in mind its measurable limitations. Firstly, it is limited by the quality and quantity of information sources available in the open. The more of them there are and the better they are qualitatively, the higher the accuracy of the reports. This necessarily leads to the conclusion that the highest effectiveness is in terms of reporting on democratic states based on civil society and with media pluralism and a culture of writing open summaries, studies, and reports. The opposite is true in authoritarian countries—here, sources are mostly scarce and need to be verified with care. Although, as the examples of Russia and Belarus show, sometimes the change in lifestyle and the development of social media in the younger generation (millennials and Generation Z) significantly outpaced the assumptions of protecting classified information, which had been in place in these countries basically since the collapse of the USSR. As a result, the services of both countries did not take into account that virtually every 20-year-old had a smartphone with internet access and spyware apps with a function to make funny videos (TikTok) or social media (Facebook, VK, Instagram) that sold privacy to advertisers. And while procedures for individual military units and construction and research companies were usually followed, they ended when monitoring the social media activity of their employees or analysing hundreds of videos of military equipment being transported on rail and road thoroughfares, leaving aside, of course, the classic imprudence of conscripts. In addition, the USSR retrospective utopia of some former officers and engineers of design companies resulted in a plethora of absolutely phenomenal and overt studies on the work of the military-industrial complex of the USSR's decline period. The fact that the "new" Russian R&D work was, in ¾ of cases, the completion of work from the USSR period facilitated the analysis despite Russia's authoritarian nature. And here we come to the second limitation: Qualitative OSINT is largely based on human factor error. If the public is properly educated and procedures in industry and regulations in the armed forces are guarded, the quality and quantity of data we receive drops dramatically. The detection time of the phenomena or threats in question is also delayed. A separate issue—a thorny one for the authors of reports—is the margin of error. The verifiability of the analyses—depending on the area studied and, above all, the quality and quantity of the information available—ranges from 60 to

[29] Business to government: exchange between business and public administration

90%. The most serious limitation of technical OSINT, however, is that it is subject to a sharp and rapid reduction in effectiveness for authoritarian countries that diagnose their vulnerability in this regard. In Russia, for example, a campaign to close down or heavily censor defence discussion forums started in May or June 2022; additional censorship of the Russian Facebook (VK) also began and TikTok was banned. The railway facility security also started to pay close attention to people taking videos and photographs. A number of other measures (restoring the soldiers' military discipline) were also taken, resulting in a decrease of more than ¾ in the amount of information available from social media. Even the first wave of mobilisation—characterised by low military discipline—did not result in a significant increase in material from the frontline or the operations themselves. Of course, the phenomenon of leaking videos taken by soldiers to the web has not been eliminated but its incidence has been reduced by an order of magnitude. The whole thing has translated into a drastic deterioration in the quantity and quality of information available.

Despite the above limitations, it is important to recognise that, nevertheless, the role of OSINT (both qualitative and quantitative) will continue to grow as a result of the online media revolution and humanity's changing lifestyles. This will be a worldwide trend, with the few exceptions being totalitarian states (North Korea) or authoritarian regimes (Iran, Russia, China, Belarus) able, through control of the ICT infrastructure (colloquially: access to the internet via nodal points and local operators controlled by the country in question) and the restrictive application of draconian laws against their own citizens, to limit the effectiveness of "open-source intelligence." However, even in countries such as Russia, Iran and China, OSINT capabilities have not been completely eliminated, which leads us to the conclusion that it will still be a useful and low-cost tool for the collection and development of information relevant to state security.